Service attributes

Service type

Lot 2b: Software as a Service (SaaS)

Service name

Service name

DBS, RtW and Identity Services

Edit

About your service

Service description

Verifile provides background screening and identity verification services to help organisations make safe, compliant hiring decisions. Their services include identity and right-to-work checks, criminal record screening, employment and education verification, credit checks, and global screening solutions delivered through a secure digital platform.

Edit

Service categories

- Applications
  - Content workflow and management
    - Content services
      - Content Sharing and Collaboration Applications
    - Capture
      - Capture
    - Document
      - Document

Edit

Multi cloud support

Yes

Edit

Service features and benefits

Service features and benefits

Service features

- Identity Verification
- Criminal Record Checks
- Employment Verification
- Education and qualification Verification
- Credit and Financial Checks
- Global Screening

- Continuous Monitoring
- Cloud-Based Platform
- Compliance Focus

Service benefits

- Improved hiring quality
- Faster, more efficient processes
- Compliance and risk mitigation
- Scaleable for global hiring
- Secure and reliable
- Better candidate experience
- Ongoing monitoring
- Integration friendly

Edit

Service scope

Add-ons and extensions

Software add-on or extension

No

Edit

Cloud deployment model

Public cloud

Edit

Service constraints

The service has minimal constraints typical of a secure, cloud-based SaaS platform. Planned maintenance and updates are carried out outside core UK business hours wherever possible, with advance notification provided. The system is accessed via a modern web browser and requires a stable internet connection; no specialist hardware is needed. Some background checks depend on third-party authorities (such as the DBS or international agencies), which may impact turnaround times outside of Verifile's control. Core support is provided during UK business hours, while the platform, dashboards, notifications and knowledge base remain available 24/7.

Edit

System requirements

- Cloud-based SaaS solution accessed via a web browser
- No specialist software installations or additional licences required
- Stable internet connection required
- Modern, supported web browser
- Compatible with standard desktops, laptops and tablets

- No requirement for specific operating systems, hardware, or virtual machines
- Buyers are expected to maintain standard endpoint security

Edit

Reselling

Supplier type

Supplier type

I’m not a reseller

Edit

User support

Email or ticketing support

Email or online ticketing support

Yes

Support response times

Emails are picked up within 48 hours of delivery thus, guaranteeing all issues are managed by an expert in a timely and efficient manner.

User can manage status and priority of support tickets

Yes

Online ticketing support accessibility

None or don’t know

Edit

Phone support

Phone support

Yes

Phone support availability

9 to 5 (UK time), Monday to Friday

Edit

Web chat support

Web chat support

Yes

Web chat support availability

9 to 5 (UK time), Monday to Friday

AI chatbot

No

Web chat support accessibility standard

None or don’t know

How the web chat support is accessible

Our web chat is designed to be accessible, inclusive, and easy to use for all users. It is available directly within the Verifile platform and website during UK business hours and does not require any additional software or downloads. The web chat is WCAG 2.1–aligned and supports common accessibility tools, including screen readers, keyboard-only navigation, adjustable text sizing, and high-contrast display settings. Users can initiate and participate in conversations using a mouse, keyboard, or assistive technologies. Through web chat, users can ask questions, receive guidance, upload information where appropriate, and be directed to relevant support or knowledge base articles. For security and privacy reasons, web chat is not used to share sensitive documents or disclose full screening results, and some complex or sensitive queries may be escalated to phone or email support.

Web chat accessibility testing

Web chat accessibility has been tested as part of our wider platform accessibility assurance aligned to WCAG 2.1 requirements. Testing includes use with common assistive technologies such as screen readers (e.g. NVDA and VoiceOver), keyboard-only navigation, and browser-based zoom and text resizing tools. We have verified that users can open the chat, read messages, type responses, and submit queries without relying on a mouse. Accessibility testing is supported by internal QA checks and feedback from users who rely on assistive technologies. Any issues identified are logged and prioritised within our development backlog, with fixes delivered through regular release cycles to ensure continuous improvement.

Edit

Onsite support

No

Edit

Support levels

Standard Support Included as part of the core service (no additional cost). Access to Client and Candidate support teams via phone, email and web chat during UK business hours. Covers day-to-day queries, order support, guidance on checks, reporting, and platform usage. Access to the online Knowledge Base and system notifications. Enhanced Support (Enhanced Service) Priced at a higher per-check rate than Standard Support. Includes all Standard Support features plus proactive, fully managed candidate support. Verifile communicates directly with candidates to chase information, resolve queries, and reduce turnaround times. Reduces operational burden on the

buyer’s internal teams. Account management and technical support All clients are assigned a dedicated Customer Success Manager (CSM) who acts as a technical account manager for service delivery, performance reviews, onboarding, and continuous improvement. Technical issues are handled by Verifile’s in-house technology and support teams, including senior engineers where required. A dedicated cloud support engineer is not required by buyers, as infrastructure and platform management are fully managed by Verifile.

Edit

Support available to third parties

Yes

Edit

How users work with your service

Browsers

Web browser interface

Yes

Supported browsers

- Microsoft Edge
- Firefox
- Chrome
- Safari

Edit

Installation

Application to install

No

Edit

Mobile

Designed for use on mobile devices

Yes

Differences between the mobile and desktop service

It uses a responsive, browser-based interface that adapts to different screen sizes and operating systems, allowing users to access core functionality on smartphones and tablets without installing a separate app. This enables users to view information, complete tasks, and manage workflows securely while on the move.

Edit

Service interface

Service interface

Yes

Description of service interface

The service interface is a secure, web-based user interface accessed through a standard browser. It provides a clear, intuitive dashboard where users can place and manage screening requests, track progress in real time, and review completed results. Navigation is role-based, ensuring users only see functions and data relevant to their permissions. The interface supports search, filtering, and reporting to help users manage high volumes efficiently. It is responsive and designed to work across desktop and mobile devices, with consistent layouts and clear status indicators to support ease of use and operational efficiency.

Accessibility standards

None or don’t know

Description of accessibility

The service is accessible through a secure, web-based interface using modern browsers on desktop, tablet, and mobile devices. Users can access the service without installing software, log in securely, place and manage requests, track progress, and download reports from any internet-connected device. The interface is responsive and role-based to support accessibility and ease of use. Users cannot access the service offline, use unsupported or outdated browsers, or bypass role-based permissions. Access is restricted to authorised users only and requires valid credentials and an active internet connection.

Accessibility testing

he service interface has been tested to support accessibility and usability for users of assistive technologies, in line with recognised best practice. Testing includes: Keyboard-only navigation to ensure all core functions can be accessed without a mouse Compatibility testing with screen readers (such as NVDA and VoiceOver) to confirm that page structure, labels, and form fields are correctly announced Use of semantic HTML and ARIA attributes to support assistive technology interpretation Contrast and readability checks to support users with visual impairments Responsive design testing to ensure accessibility across desktop and mobile devices In addition, accessibility considerations are incorporated into design and development reviews, and feedback from users is used to improve usability. While the service is not positioned as a specialist assistive-technology product, it is designed to align with WCAG 2.1 AA principles where reasonably practicable.

Edit

User support

User support accessibility

None or don’t know

Edit

API

API

Yes

What users can and can't do using the API

Users can interact with the Verifile service via an API to automate and streamline background screening workflows, particularly where integrations with HR or applicant tracking systems (ATS) are required. Through the API, users can set up the service by integrating their HR or ATS platform with Verifile’s system, enabling screening orders to be created automatically rather than manually through the web portal. This allows candidate details to be securely transferred, orders to be placed, and invitation emails to be triggered without additional user intervention. Bulk ordering can also be supported through API-driven processes, following Verifile’s defined data structure. Using the API, users can submit new screening requests, pass candidate information, and manage order creation at scale. Changes are typically made by submitting updated or additional orders rather than editing completed checks. This ensures data integrity and auditability throughout the screening process. There are some limitations to API usage. Configuration of accounts, users, permissions, packages, and reporting settings is not self-managed via the API and is handled through the Verifile onboarding and customer success teams. Bulk submissions must follow a fixed data schema and cannot be customised by buyers. API integrations are subject to technical evaluation.

API documentation

Yes

API documentation formats

HTML

API sandbox or test environment

Yes

Edit

Customisation

Customisation available

Yes

Description of customisation

Users can customise the Verifile service to align with their organisational structure, recruitment workflows, and compliance requirements, while core platform controls remain standardised to maintain security and data integrity. What can be customised Customers can customise account and sub-account structures, user roles and permissions, screening packages, candidate

communication templates, reporting outputs, notification settings, and integration methods. Screening packages can be configured to be role-specific, allowing different checks to be applied to different job types or locations. Reporting and dashboards can be tailored to show volumes, turnaround times, and performance metrics relevant to the buyer. How users can customise Customisation is delivered through a combination of self-service configuration within the platform and guided setup during onboarding. Buyers can request changes such as new packages, reporting formats, or workflow adjustments through their Customer Success Manager. Integrations can also be configured to align with the buyer's HR or ATS systems. Who can customise Customisation is controlled through role-based access. Authorised buyer administrators can request or apply permitted changes, while more complex or compliance-sensitive configurations are implemented by Verifile's onboarding, technical, or Customer Success teams to ensure accuracy and regulatory compliance.

Edit

Onboarding and offboarding

Getting started

From the outset, each client is assigned a dedicated onboarding specialist who works closely with them to understand their organisation's requirements, risk profile, and hiring processes. This begins with a kick-off meeting to define screening needs, timelines, user roles, and any sector-specific compliance requirements. Verifile then configures the platform to match the client's setup, including account structures, user permissions, customised screening packages, reporting preferences, and candidate communication templates. Where required, Verifile can also support system integrations with HR or applicant tracking systems to streamline workflows and reduce manual effort. Comprehensive training is provided as part of onboarding, ensuring users are confident in placing orders, tracking progress, reviewing results, and generating reports. Training sessions can be delivered live, recorded for future reference, and repeated when new users join. Throughout this phase, clients benefit from regular check-ins and progress updates to ensure a smooth transition to live service. Once onboarding is complete, responsibility is handed over to a dedicated Customer Success Manager, who provides ongoing support, optimisation guidance, and regular service reviews. This approach ensures users can start using Verifile quickly while receiving long-term support to maximise value and compliance.

Edit

Documentation

Service documentation

Yes

Documentation formats

- HTML

- PDF

Documentation accessibility standard

None or don’t know

How the documentation is accessible

Onboarding and off-boarding documentation is made accessible through a combination of digital resources, guided support, and ongoing access controls to ensure users can easily find and use the information they need at every stage of the service lifecycle. During onboarding, clients are provided with clear, structured documentation that is shared digitally. This includes written guides, PDFs, and training materials that explain how to use the platform, place and manage orders, interpret results, and configure settings such as user permissions and reporting. Much of this content is available through an online knowledge base, allowing users to access it 24/7 from any location. Live or recorded training sessions complement the documentation, ensuring different learning preferences are supported. Access to onboarding documentation is role-based, meaning administrators and users only see information relevant to their responsibilities. Documentation remains available after go-live, so users can revisit guidance whenever needed or share it with new team members. Off-boarding documentation is also provided digitally and outlines processes for closing accounts, managing user access, handling data retention or deletion, and meeting compliance obligations. This information is typically shared directly with authorised client contacts and supported by the Customer Success team to ensure clarity and continuity.

Edit

End-of-contract data extraction

Users can extract their data from Verifile through a controlled, secure off-boarding process designed to ensure data ownership, continuity, and compliance. Prior to contract termination, authorised client users are given the opportunity to export required data directly from the Verifile platform. This typically includes candidate records, screening results, final reports, and management information. Data can be extracted in commonly used digital formats such as PDF reports and CSV files, allowing organisations to store the information within their own systems for audit, compliance, or record-keeping purposes. If clients require more structured or comprehensive datasets, Verifile can support bespoke data exports upon request. These are coordinated with the client’s designated contact to ensure the correct scope, format, and timeframe are agreed in advance. Throughout this process, access controls remain in place so only authorised users can retrieve data. Once data extraction has been completed, Verifile follows agreed data retention and deletion instructions, aligned with contractual terms, legal obligations, and GDPR requirements. Certain records (such as right-to-work evidence) may be retained for legally mandated periods, after which they are securely deleted or anonymised. The Customer Success team supports clients throughout off-boarding to ensure data is transferred smoothly, securely, and without disruption.

Edit

End-of-contract process

Verifile follows a structured and controlled off-boarding process to ensure a smooth, secure, and compliant conclusion of the service. The process begins with coordination between the client and Verifile's Customer Success team to agree timelines, responsibilities, and any final requirements. This includes confirming the contract end date, access arrangements, and data handling instructions. Before service access is closed, authorised users are given the opportunity to extract their data from the Verifile platform. This may include candidate records, screening reports, audit trails, and management information, typically provided in standard digital formats such as PDF and CSV. Verifile can support bespoke data exports to meet specific organisational or regulatory requirements. Once data extraction is complete, system access is gradually removed in line with agreed timelines to prevent unauthorised use. Verifile then manages data retention and deletion in accordance with contractual terms, GDPR, and legal obligations. Certain records, such as right-to-work documentation, may be retained for statutory periods before being securely deleted or anonymised. Throughout the off-boarding phase, Verifile provides clear communication and support to ensure continuity, compliance, and minimal disruption. This approach ensures clients retain ownership of their data while maintaining high standards of security and regulatory compliance at contract end.

Edit

Data importing and exporting

Data export approach

Users export data from Verifile through a secure and controlled process at or before contract end. Authorised users can download screening reports, candidate records, and management information directly from the platform in standard formats such as PDF and CSV. For larger or more complex requirements, Verifile can provide tailored data exports upon request, agreed in advance with the client. All exports are subject to role-based access controls to ensure data security. Once exports are completed, access is removed in line with off-boarding timelines and compliance requirements.

Edit

Data export formats

Data export formats

- CSV
- Other

Other data export formats

- PDF
- Excel compatible files

Edit

Data import formats

Data import formats

CSV

Edit

Analytics

Metrics

Service usage metrics

Yes

Metrics types

Verifile can provide service usage metrics as part of its reporting and management information capabilities. Common usage metrics that can be provided include: - Number of checks ordered: total and by type (e.g. identity, DBS, employment). - Turnaround times: average time to complete checks, by check type. - Status tracking: counts of orders in progress, completed, pending, or returned for action. - User activity: which users placed orders and when. - Volume trends: usage over time (daily, weekly, monthly). - Compliance metrics: e.g. completion rates within SLA windows.

Reporting types

- Real-time dashboards
- Regular reports

Resource tagging

No

FOCUS resource tagging

No

Edit

Scaling

Independence of resources

Verifile ensures users are not impacted by other customers' demand through scalable cloud-based infrastructure and robust operational controls. The SaaS platform is designed to scale automatically during peak usage, preventing performance degradation. Workloads are balanced across specialist and cross-skilled teams to maintain service levels, even during high-volume periods. Continuous monitoring against SLAs allows issues to be identified and resolved early. In addition, strict data segregation and role-based access controls ensure each client's activity and data remain isolated. This approach delivers consistent performance, reliability, and security for all users.

Edit

Public sector networks

Public sector networks

Connection to public sector networks

Yes

Connected networks

Other

Other public sector networks

- Disclosure & Barring Service
- Disclosure Scotland
- Access NI

Edit

Data-in-transit protection

Protection between networks

Data protection between buyer and supplier networks

Private network or public sector network

Edit

Protection within your network

Data protection within supplier network

Other

Other protection within supplier network

Verifile protects data through a layered security approach. Its cloud-based SaaS platform is hosted on Microsoft Azure and uses secure virtual networks, firewalls, and continuous monitoring. All data is encrypted both in transit and at rest. Access is restricted through role-based access controls and multi-factor authentication, with activity logging and audit trails in place. Client data is logically segregated to prevent cross-access. Verifile's security framework is independently accredited to ISO 27001, Cyber Essentials Plus, and NSI Gold, ensuring strong governance, regular testing, and continuous improvement of network and data protection controls.

Edit

Asset protection

Data storage and processing locations

Knowledge of data storage and processing locations

Yes

Data storage and processing locations

United Kingdom

User control over data storage and processing locations

No

Edit

Datacentre security standards

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Penetration testing

Penetration testing frequency

At least once a year

Penetration testing approach

In-house

Edit

Protection of data at rest

Protecting data at rest

Encryption of all physical media

Edit

Data sanitisation process

Data sanitisation process

Yes

Data sanitisation type

- Deleted data can’t be directly accessed / Cryptographic Erasure
- Data Erasure
- Explicit overwriting of storage before reallocation / Secure Erase

Edit

Equipment disposal approach

A third-party destruction service

Edit

Availability and resilience

Guaranteed availability

Verifile delivers a high level of service availability designed to support business-critical screening activities and minimise disruption for users. The platform is provided as a cloud-based SaaS solution hosted on resilient infrastructure, with built-in redundancy and fault tolerance to ensure

consistent access. Availability is continuously monitored to identify and address potential issues before they impact users. Verifile operates in line with defined service level agreements (SLAs) that set clear expectations around platform uptime and performance. These SLAs are supported by proactive system monitoring, automated alerts, and on-call technical support to enable rapid response and resolution in the event of an incident. Maintenance activities are planned carefully and, wherever possible, scheduled outside of core operating hours to reduce impact on customers. Business continuity and disaster recovery arrangements are embedded within the service and aligned with ISO 22301. These measures ensure, in the event of a major incident, services can be restored quickly and data integrity maintained. Regular testing of continuity and recovery plans provide assurance our controls remain effective. Operational capacity is managed to handle fluctuations in demand without degrading performance.

Edit

Approach to resilience

Our service is designed to be resilient at both the application and data-centre level, ensuring continuity, reliability, and rapid recovery from disruption. It is delivered as a cloud-based SaaS platform hosted in secure, resilient data centres that are built with high availability in mind. Our data centres incorporate redundant power supplies, network connectivity, cooling systems, and physical security controls, ensuring continued operation . Within the data centre environment, the platform uses redundant compute, storage, and networking to eliminate single points of failure. Data is replicated and securely backed up to protect integrity and availability. Automated monitoring and alerting operate 24/7, enabling rapid detection and response to infrastructure or performance issues. Resilience is further strengthened through business continuity and disaster recovery controls, aligned with ISO 22301. These include defined recovery objectives, regular backup testing, and documented recovery procedures to ensure services can be restored quickly following a major incident. Operational resilience complements the technical design. Capacity planning ensures the platform can handle demand spikes without degradation, while cross-skilled teams and controlled change management reduce operational risk. Together, resilient data-centre infrastructure, redundant system design, proactive monitoring, and tested recovery processes ensure the service remains stable, secure, and available under adverse conditions.

Edit

Outage reporting

The service reports outages and service issues through multiple transparent communication channels, ensuring users are informed promptly and consistently. For real-time visibility, the service provides a public service status dashboard that displays current system availability, performance, and any active incidents. This dashboard allows users to independently check service health at any time without needing to contact support. When an incident occurs, the dashboard is updated with clear status indicators, impact summaries, and progress updates until resolution. In addition, automated email alerts are issued to designated client contacts when significant outages

or service degradations are identified. These alerts provide details on the nature of the issue, affected services, expected impact, and ongoing remediation actions. Follow-up communications are sent as the incident progresses and once normal service is restored. For integrated customers, the service can also expose status information via API, enabling organisations to consume service health updates within their own monitoring or IT service management tools. This supports automated awareness and internal escalation where required. All incidents are logged and reviewed internally, with post-incident analysis used to prevent recurrence. Planned maintenance is communicated in advance through the same channels to minimise disruption.

Edit

Governance

Named board-level person responsible for service security

Yes

Edit

Security governance

Software Security Code of Practice

Yes

Security governance certified

Yes

Security governance standards

ISO/IEC 27001

Edit

Information security policies and processes

Our service follows a comprehensive Information Security Policy and supporting processes designed to protect the confidentiality, integrity, and availability of data throughout its lifecycle. These policies are governed by a formal Information Security Management System (ISMS) aligned with ISO/IEC 27001, ensuring a structured, auditable, and continuously improving approach to security. Our Information Security Policy defines roles and responsibilities, including board-level oversight, and sets out requirements for risk management, access control, data protection, incident response, and compliance with legal and regulatory obligations such as GDPR. Supporting procedures translate the policy into practice, covering areas such as secure system configuration, encryption, identity and access management, and logging and monitoring. Risk assessments are conducted regularly to identify threats and vulnerabilities, with mitigation actions tracked and reviewed. Access to systems and data is controlled using role-based access, least-privilege principles, and multi-factor authentication where appropriate. All data is encrypted at rest and in transit, and client data is logically segregated. Incident management processes define how security events are detected,

escalated, investigated, and resolved, including notification and post-incident review. Regular internal audits, independent external audits, staff security training, and continuous monitoring ensure policies remain effective and up to date.

Edit

Operational security

Configuration and change management standard

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Configuration and change management approach

Our service follows a formal configuration and change management process aligned with ISO/IEC 27001 and ITIL best practice. Secure baseline configurations are defined, documented, and version-controlled to ensure systems remain consistent and protected. Any changes to applications, infrastructure, or security settings are logged, risk-assessed, and approved by authorised personnel. Changes are tested in development and pre-production environments before release, with rollback plans in place to minimise disruption. Emergency changes follow an accelerated but controlled process. This approach ensures security, stability, traceability, and continuous improvement across the service.

Edit

Vulnerability management type

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Vulnerability management approach

Our service follows a formal vulnerability management process aligned with ISO/IEC 27001 and security best practice. Vulnerabilities are identified through automated scanning, continuous monitoring, and regular security testing. Each issue is assessed based on severity and risk, then prioritised for remediation. Patches and fixes are applied within defined timeframes, with critical vulnerabilities addressed urgently. All remediation activities are tracked and implemented through controlled change management processes. Continuous monitoring and review ensure vulnerabilities are resolved effectively and inform ongoing security improvements.

Edit

Protective monitoring type

Complies with a recognised standard, for example CSA CCM v4.0 or SSAE-18 / ISAE 3402

Edit

Protective monitoring approach

Protective monitoring is implemented to detect, analyse, and respond to security events in real time. The service uses continuous logging and monitoring across applications, networks, and infrastructure to identify suspicious or abnormal activity. Security alerts are generated automatically and reviewed by authorised personnel, enabling rapid investigation and response. Logs are securely stored and retained in line with compliance requirements to support audit and forensic analysis. Monitoring tools are configured to detect threats such as unauthorised access, configuration changes, and system anomalies. This approach ensures early detection of risks and supports effective incident management.

Edit

Incident management type

Complies with a recognised standard, for example, CSA CCM v4.0 or ISO/IEC 27035:2011 or SSAE-18 / ISAE 3402

Edit

Post-quantum cryptography secure

Yes

Edit

Incident management approach

We operate a formal incident management process aligned with ISO/IEC 27001 and ITIL best practice. Pre-defined response procedures are in place for common incidents such as service outages, security events, and access issues, with clear roles, escalation paths, and recovery steps. Users can report incidents via email, phone, or the support portal, and all incidents are logged and prioritised in a central system. Automated monitoring also raises incidents. For significant events, we provide timely updates and a post-incident report detailing impact, root cause, actions taken, and preventative measures.

Edit

Staff security

Staff security clearance

Staff screening performed which conforms to BS7858:2019

Edit

Government security clearance

Up to Baseline Personnel Security Standard (BPSS)

Edit

Secure development

Approach to secure software development best practice

Independent review of processes (for example CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001 or CSA CCM v4.0)

Edit

Identity and authentication

User authentication

User authentication needed

Yes

User authentication

- Multi-Factor Authentication (MFA)
- Username or password

Edit

Access restrictions in management interfaces and support channels

Access to management interfaces and support channels is restricted using layered security controls. Role-based access control ensures users can only access functions relevant to their role, following the principle of least privilege. Multi-factor authentication is enforced for privileged access, and permissions are reviewed regularly. All access and actions are logged and monitored for audit and security purposes. Support channels are limited to verified users, with identity checks performed before sensitive actions or data are discussed. Support staff access to customer data is controlled, role-based, and logged. These controls ensure secure, auditable access aligned with best practice.

Edit

Access restriction testing frequency

At least once a year

Edit

Management access

Management access authentication

- Multi-Factor Authentication (MFA)
- Username or password

Edit

Audit information for users

Audit for buyers' users' actions

Access to user activity audit information

Users have access to real-time audit information

How long user audit data is stored for

User-defined

Edit

Audit for suppliers' users' actions

Access to supplier activity audit information

Users have access to real-time audit information

How long supplier audit data is stored for
User-defined

Edit

How long system logs are stored for

User-defined

Edit

Pricing

Discount for educational organisations

No

Edit

Free or trial versions

Free trial available
No