Wonde MyLogin

Service Definition Document

mylogin

Wonde MyLogin

"..The time saved by the teachers is significant throughout their lessons and during lesson preparation. This has led to an increase in confidence of using technology across 29 schools and has revolutionised the way we now use technology across the Trust...".
Peter Bradburn, Head of IT, Aspire Academy Trust

What is MyLogin?

Wonde MyLogin is a secure, cloud-based identity and access management (IAM) service designed for education and public sector environments. It provides a single, centrally managed authentication layer that enables users to access approved applications and services using one set of credentials, supported by robust security controls and audit capabilities.

MyLogin replaces multiple separate application logins with a single authentication service managed by the organisation. Administrators manage users, roles and access rules in one place, rather than maintaining separate credentials across systems. Authentication policies, including multi-factor authentication, are applied consistently, and user access and administrative actions are recorded in audit logs.

The service is delivered as a fully managed Software as a Service (SaaS) solution and is used at scale across thousands of educational organisations.

Further information is available at www.mylogin.com/mylogin/

Core functionality

MyLogin provides the following core capabilities:

- Single sign-on (SSO) across connected applications and services
- Centralised user account lifecycle management, where user creation, updates and deactivation are automatically synchronised from the organisation's MIS

- Role-based access control to ensure users only access approved systems and functions
- Support for multi-factor authentication (MFA) to strengthen account security
- Secure credential handling and encrypted storage
- Administrative oversight of application access and authentication policies
- Comprehensive audit logging of authentication events and administrative actions

Applications are made available to users through an approved access layer, ensuring access is controlled, consistent and auditable.

Data backup, restore and disaster recovery

Wonde maintains regular, point-in-time backups of all data processed by the MyLogin service. This includes identity records, authentication data and audit logs required for the secure operation of the service.

If an organisation revokes access or the service is no longer required, access to operational data is disabled. Data is retained in line with Wonde's data retention policies and may be deleted or anonymised in accordance with contractual or regulatory requirements. Backup, restore and disaster recovery processes are tested and maintained as part of Wonde's information security management system.

Onboarding and offboarding support

Wonde provides full onboarding and offboarding support throughout the service lifecycle. This includes:

- Initial service setup and configuration
- Support with application integration and access configuration
- Administrator guidance and documentation
- Ongoing account and service management support
- Secure offboarding and controlled data deletion at contract end

Buyers are provided with a secure administrative interface to manage users, monitor service status and access documentation. Service performance and support levels are managed against agreed service targets.

Service constraints and customisation

MyLogin is a standardised SaaS service designed to deliver consistent security and reliability at scale.

Administrators can configure the service within defined parameters, including user roles, access permissions, authentication methods and approved applications. Core security controls, minimum authentication standards and audit logging requirements are enforced centrally and cannot be reduced below defined baselines.

The administrative interface is browser-based and accessed via supported modern web browsers. No local software installation is required.

Scheduled maintenance is carried out outside of normal working hours wherever possible and with advance notice to customers.

Service levels, performance and availability

MyLogin is designed for high availability and resilience. The service is provided with a target availability of 99.95%.

The service is hosted on cloud infrastructure that automatically scales to meet demand, ensuring consistent performance during peak usage. Service levels and any applicable service credits are defined contractually.

Support

MyLogin is supported by Wonde's UK-based, in-house support team. Support is available throughout the service lifecycle and includes access to experienced technical and account support staff familiar with education and public sector environments.

Support channels include:

- Telephone
- Email
- Web-based support
- Online self-service documentation and guidance

Integration and configuration guidance is available for supported systems and applications.

Technical requirements

MyLogin is a cloud-based service accessed via a web browser. The service supports current versions of major browsers, including Chrome, Microsoft Edge, Firefox and Opera, on Windows, macOS and supported mobile platforms.

A reliable internet connection is required. No specialist hardware or local infrastructure is required to use the core MyLogin service. Some optional features, such as device-based access controls, may have additional configuration or device requirements.

Security

Wonde operates a comprehensive information security management framework. The organisation is certified to ISO/IEC 27001 and Cyber Essentials Plus, with independent audits covering information security controls, risk management, change management and operational processes.

Security measures include:

- Encryption of data in transit and at rest
- Role-based access controls and restricted administrative permissions
- Multi-factor authentication for administrative access
- Continuous monitoring and audit logging
- Regular security testing and review

These controls ensure that MyLogin meets public sector security and data protection expectations, including compliance with UK GDPR requirements.