Authentication & Authorization Service Documentation

Summit Digital Solutions, Inc.

Version 2.4 | Last Updated: December 15, 2023

Document Classification: Confidential

1. Overview and Scope

1. This Authentication & Authorization Service Documentation ("Documentation") describes the security infrastructure, protocols, and procedures implemented by Summit Digital Solutions, Inc. ("Company") for identity management and access control within the Peak Performance Platform(TM) and related enterprise systems.

2. This Documentation is considered confidential and proprietary information of the Company and is subject to the terms of applicable non-disclosure agreements.

2. Authentication Architecture

1. **Core Authentication Framework**

- Implementation of OAuth 2.0 and OpenID Connect protocols
- Multi-factor authentication (MFA) support using TOTP and FIDO2
- JSON Web Token (JWT) based session management
- Encrypted credential storage using AES-256 encryption

2. **Identity Providers**

- Native authentication provider
- SAML 2.0 federation support
- Integration with enterprise identity providers:
- Microsoft Azure AD
- Okta
- OneLogin
- Custom LDAP implementations

3. Authorization Model

1. **Role-Based Access Control (RBAC)**

- Hierarchical role structure
- Custom role definition capability
- Granular permission sets
- Role inheritance patterns

2. **Resource Access Policies**

- Resource-level permissions
- Attribute-based access control (ABAC)
- Dynamic policy evaluation
- Contextual access rules

4. Security Standards Compliance

1. The authentication and authorization services maintain compliance with:

- SOC 2 Type II
- ISO 27001:2013
- GDPR
- CCPA
- NIST Cybersecurity Framework

2. **Audit Logging**

- Comprehensive authentication event logging
- Access attempt tracking
- Policy modification audit trail
- System configuration change logging

5. Technical Specifications

1. **API Security**

- REST API security implementation
- API key management
- Rate limiting
- Request signing

2. **Encryption Standards**

- TLS 1.3 for all communications
- At-rest encryption for credentials
- Key rotation procedures
- Hardware Security Module (HSM) integration

6. Integration Capabilities

1. **Enterprise System Integration**

- Standard protocol support (SAML, OAuth, OIDC)
- Custom connector framework
- API-based integration
- Legacy system support

2. **Peak Performance Platform(TM) Integration**

- Native integration with platform components
- Unified authentication experience
- Single sign-on capabilities
- Session management

7. Disaster Recovery and Business Continuity

1. **High Availability Configuration**

- Active-active deployment
- Geographic redundancy
- Automatic failover
- Load balancing

2. **Backup and Recovery**

- Daily credential store backups
- Configuration backups
- 15-minute RPO
- 1-hour RTO

8. Service Level Agreements

1. **Availability**

- 99.99% uptime guarantee
- Maximum 5-minute authentication service downtime
- 24/7 monitoring and support

2. **Performance**

- Authentication request processing: <500ms
- Authorization decision rendering: <200ms
- Token validation: <100ms

9. Legal Disclaimers

1. This Documentation is provided "as is" without warranty of any kind, either express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

2. The Company reserves the right to modify this Documentation and the described services at any time without prior notice.

10. Document Control

1. **Version History**

- v2.4 (Current) - December 15, 2023
- v2.3 - September 30, 2023
- v2.2 - June 15, 2023
- v2.1 - March 1, 2023

2. **Approval**

APPROVED AND ADOPTED by Summit Digital Solutions, Inc.

By:

Name: Michael Chang

Title: Chief Technology Officer

Date: December 15, 2023

By:

Name: James Henderson

Title: Chief Digital Officer

Date: December 15, 2023