Safety Instructions

Stay safe if you see these signs ⚠⛔
This indicates an attempt to break the security chain. The security chain must function within 30 seconds.

Stop work if you see this sign.
This indicates a broken security chain. The security chain must function within 30 seconds.
"⚠⛔🔒"

Table of Contents:

---

1. Introduction

The product enables secure session management, data handling, and network traffic rate limiting. This manual will guide you through the key system functions.

2. Standards Compliance

Our product is based on international standards, ensuring compliance with the highest quality and security norms.

3. Data Capacity Management

The application has a static database size of 16,532,000 bytes. This is the total value resulting from the user's identification capacity and data limits. Below are the capacity details for a single identity:
• User Identification: 148 bytes.
• Data Limit: One target and one group per session.
• Dictionary Limit: 1024*8 bytes per target and group.

4. Request Rate Limiting

The system uses the Token Bucket algorithm to limit the number of requests sent by clients within a given time interval. This allows traffic management and prevents server overload.

Key Parameters:
• Interval Time: Default 4 seconds.
• Average Number of Requests: The client can send 16 requests per time interval.

• Bursting Value: 4 (allows for short-term exceeding of the average number of requests in case of sudden traffic spikes).
• Concurrent Request Limit: The client can perform up to 64 simultaneous requests.

---

5. Security

Data and system security are critical to ensuring user data protection and stability.

Key Principles:

1. **Communication Encryption:**
   o All data transmitted between the server and the client is encrypted. Using encrypted communication ensures that third parties do not intercept data.
2. **Identity Security:**
   o User identities are stored securely, following current data protection standards. Each user has a unique identity, and identification data is processed in accordance with GDPR and other privacy regulations.
3. **Authorization and Authentication Mechanisms:**
   o The system requires appropriate user authentication mechanisms. Each user has a unique token that meets security standards.
4. **Access Limitation:**
   o Users have access only to the data and resources necessary for their tasks.
5. **Protection Against Attacks:**
   o The system is resistant to DoS (Denial of Service) and DDoS (Distributed Denial of Service) attacks, which can overload the server and limit service availability.
6. **Data Storage and Archiving:**
   o Important data, such as passwords, are always hashed using secure algorithms. Additionally, sensitive data is encrypted during transmission and stored on servers (initial installation always consists of 0 sensitive data – it is possible due to cryptographic chain nature).
   o Identity protection, regular archiving, and creating data backups are crucial to prevent data loss due to system failure or attacks. The system uses two independent databases, eliminating the need for manual archiving and backups, as one of the databases is embedded in the browser—acting as a "Main Ledger" similar to an accounting system called "Double-Entry Bookkeeping."
   Traditional accounting systems operate on double-entry bookkeeping, where each financial transaction impacts at least two accounts (debit in one and credit in another). This ensures that the accounting equation (Assets = Liabilities + Equity) always remains balanced.

---

7. Monitoring and Logging:

o The system monitors its parameters to detect unauthorised activities. Alerts are triggered with the messages "⚠⛔" and "⚠⛔🔒," indicating a warning or security breach. This approach avoids text messages and uses universal symbols. It occurs when the secure event loop is broken due to connection loss, exceeding the set limit, which blocks attacks on data transmission based on cryptography. Without this protection, cryptography-based attacks would be possible.

In summary, data and system security must be prioritised, and adherence to the above principles will ensure the protection of both user data and system stability.