INTELLECTUAL PRODUCT PROPERTY CERTIFICATE

Secure Panel – Interactive Control Panel for Secure Web Access

Flag and coat of the country in whose jurisdiction the commercial register of intellectual works operates

Short description

The application is a secure web-based control panel that provides flexible access to a secure authentication and user management system. The panel allows administrators to securely manage access, store accounts, and use advanced security technologies, including CSRF, CORS, OAuth, Reverse Proxy, and IP Request Limiting.

This solution is focused on:
• IT infrastructures requiring strict access control.
• Corporate networks that require secure management of internal resources.
• Web services and APIs that require centralized authentication.

Key features:
User authentication and management
• JWT and session tokens support.
• Multi-factor authentication (2FA, Google Authenticator).
• Roles and access rights (Admin, User, Support, Guest).
• Logging user actions.
Safety and control
• Fully protected CSRF and CORS framework for working behind a proxy.
• Rate Limiting to prevent DDoS attacks.
• Integration with Redis Cache to optimize work and session storage.
Flexibility and extensibility
• REST API for interaction with other services.
• Possibility of integration with external APIs (MailCow, OAuth, Active Directory).
• Docker support for quick deployment and scalability.
Proxying and balancing
• Support for working behind a Reverse Proxy (Nginx, Traefik).
• Support for HTTPS and SSL.
• Dynamic user management behind the load balancer.

This application is not just a control panel, but an innovative web access system that takes into account all aspects of modern attacks. Thanks to the combination of CSRF protection, API access, integration with Redis and Reverse Proxy, the product is a

proprietary secure web access system with intelligent user session management. Secure Panel is a unique security management solution that can be developed into a cloud-based platform or an on-premise solution with a commercial license.

Full description

“Secure Panel” is an intelligent web access and security control system designed to manage authorization, authentication and security in cloud and on-premises environments.

Product is focused on:

Corporate networks with high security requirements.
SaaS platforms for API security.
DevOps and CI/CD systems that require flexible access control.
Web applications with authentication and data security integration.

Basic functionality

Intelligent authentication system

- Support for multi-factor authentication (MFA).
- Integration with OAuth, LDAP and Active Directory.
- Ability to use WebAuthn and FIDO2.
- Support for separation of user roles and rights.

Access control via API

- Support for JWT and time-limited tokens.
- Secure inter-service interactions via API.
- Request control based on IP, User-Agent and geolocation.
- Automated token update and rotation.

Web Application and API Protection

- Comprehensive CORS protection with dynamic settings.
- CSRF control module with automatic token validation.
- Intelligent request limiting mechanism (Rate Limiting).
- Built-in abnormal activity detection and attack prevention.

Flexibility and scalability

- Full containerization with Docker/Kubernetes support.
- Ability to work behind Reverse Proxy (Nginx, Traefik).
- Automatic horizontal scaling for load.
- Integration with logging and monitoring systems (ELK, Prometheus).

Centralized management and audit

- Logging of all user actions and API requests.
- Visualization of logs in a flexible interface or via API.
- Automatic notification of suspicious activity.
- Complete confidentiality and compliance with GDPR standards.

Technical features

1. Dynamic CORS management

The system automatically configures valid request sources (origins) and manages security policies without the need for static configuration, which allows transparent integration of the service into various infrastructures.

2. Adaptive CSRF protection

The proprietary mechanism for automatic token generation and validation works even behind a reverse proxy, providing protection against data substitution and attacks through fake referrers.

3. Intelligent API Firewall

The technology of smart restriction of API requests allows you to block suspicious IP addresses and bots by analyzing user behavior, request headers and statistics of abnormal actions.

4. Hybrid authentication system

The system allows you to dynamically switch between local authorization modes, integration with corporate AD/LDAP and external OAuth providers.

5. Autonomous Caching and Load Balancing

Proprietary smart caching technology in Redis/Memcached allows you to reduce the load on the server while providing instant access to critical authentication data

Potential development areas

Commercial use

- Subscription-based SaaS platform for secure API access.
- On-premise version for enterprise servers with high security.
- Integration with cloud providers (AWS, GCP, Azure).

Advanced features

- Additional protection against DDoS and abnormal behavior.
- Use of AI for predictive security.
- Support for biometric authentication.

Differences from existing technologies

“Secure Panel” is an innovative web security system that not only provides authorization, but intelligently manages access in accordance with modern data protection standards.

The model includes:

Intelligent CORS and CSRF management

Hybrid authentication system

Automatic API protection from attacks and substitutions

Flexibility and integration with corporate services

Key innovations:

Hybrid CSRF/CORS protection compatible with proxies.

Dynamic session management, working with Redis and caching.

Intelligent API-protected interaction, without loss of speed.

Authorization control through rate limits + JWT.

Purpose and expected outcome

“Secure Panel” is an intelligent web access and security control system designed to manage authorization, authentication and security in cloud and on-premises environments.

Product is focused on:

Corporate networks with high security requirements.
SaaS platforms for API security.
DevOps and CI/CD systems that require flexible access control.
Web applications with authentication and data security integration.

Way of implementing the technology

Secure Panel technology can be implemented through the synergy of existing technologies described above in the text of the copyright certificate.

Author

wed20@protonmail.com
Author ID 233202411261311280000000001