PROTECTIMUS

Technical Overview

Version 1.0.4 EN
dated 07 April 2026

Contents

Solution Overview

Protectimus is a multi-factor authentication (MFA) platform designed to secure access to applications, systems, and infrastructure across organizations of any size.

The platform provides a centralized authentication layer that processes authentication requests and enforces security policies across company environments.

It supports a wide range of authentication scenarios, including multi-factor authentication, passwordless access, and directory-integrated authentication (DSPA).

Multiple authentication methods and OTP delivery channels are supported, including mobile applications, hardware tokens, push notifications, messaging platforms, SMS, and email.

The solution is available in both cloud-based (SaaS) and on-premise deployment models, providing flexibility in infrastructure and data control.

Why Protectimus

Protectimus enables organizations to implement strong multi-factor authentication without redesigning existing systems or authentication flows.

Key advantages include:

- **Flexible deployment without architectural constraints**
  Available as both a cloud-based service and an on-premise platform, allowing organizations to meet security, compliance, and data residency requirements without changing authentication workflows.
- **Seamless integration with existing systems**
  Integrates with Active Directory, LDAP, VPNs, and enterprise applications without requiring client-side changes or system redesign.
- **Directory-native authentication (DSPA)**
  Extends existing authentication flows by replacing static passwords with dynamic OTP credentials and enabling OTP-based passwordless authentication.
- **Advanced transaction security (CWYS)**
  Verifies authentication requests using contextual data, protecting critical operations against phishing and man-in-the-middle attacks.

- **Comprehensive token ecosystem**
  Supports mobile authenticators, hardware tokens, push authentication, messaging platforms, SMS, and email, ensuring compatibility with diverse user environments and security policies.
- **Scalable architecture for enterprise environments**
  Designed for distributed deployments, clustering, and high availability, ensuring reliable operation in mission-critical systems.

Typical Use Cases

Protectimus secures access across a wide range of enterprise scenarios, from remote workforce authentication to protection of critical business operations.

Typical use cases include:

- **Secure remote access (VPN, RDP)**
  Enforces multi-factor authentication for employees connecting via VPNs and remote desktop solutions, ensuring secure access to corporate networks.
- **Privileged and administrative access protection**
  Adds an additional layer of security for administrators and high-risk accounts, reducing the risk of credential compromise and unauthorized access.
- **Web applications and SSO environments**
  Protects access to web applications, identity providers, and Single Sign-On (SSO) systems such as ADFS and Office 365.
- **Financial and transaction-based systems**
  Secures sensitive operations using transaction verification (CWYS), ensuring that critical actions are validated and protected from manipulation.
- **Infrastructure and network access (RADIUS-based systems)**
  Provides MFA for network devices, including firewalls, Wi-Fi, VPN gateways, and other RADIUS-compatible systems.

System Features

System Capabilities

Protectimus is designed to operate reliably across complex and distributed IT environments, supporting both cloud-based (SaaS) and on-premise deployment models.

The platform supports deployment on Linux, FreeBSD, and Windows environments and integrates seamlessly with modern enterprise infrastructure and authentication workflows.

The system supports the current and older versions of these popular browsers: Google Chrome, Mozilla Firefox, and Internet Explorer.

Protectimus enables geographically distributed deployments, operating either as a globally available cloud service or as a clustered, multi-node system within a customer's infrastructure.

High availability is achieved through clustering, node replication, failover mechanisms, and load balancing. In distributed environments, the system ensures continuity through quorum-based node management and consistent data replication.

A wide range of authentication methods and OTP delivery channels is supported, allowing organizations to adapt authentication strategies to specific security, usability, and cost requirements.

Algorithms Used to Generate One-Time Passwords

Protectimus uses industry-standard algorithms for one-time password generation, ensuring security, reliability, and interoperability across different systems and authentication methods.

Supported algorithms include:

- HMAC (RFC 2104)
- HOTP (RFC 4226)
- TOTP (RFC 6238)
- OCRA (RFC 6287)

These algorithms are defined by the OATH (Initiative for Open Authentication) standards and are widely adopted in modern multi-factor authentication solutions.

Technology Stack

Protectimus is built using proven and widely adopted technologies, ensuring stability, performance, and maintainability. The platform architecture supports scalability, high availability, and efficient resource utilization.

#	Tools	Name (Version)
1	Foundation	Java 21
2	Web/App Server	Undertow
3	Framework	Spring 6
4	GUI	Vue 3
5	ORM	Spring JDBC
6	Database	Postgres SQL 16
7	Building	Maven 3
8	High-performance, distributed memory object caching system	Redis
9	Application Load Balancing and Content Caching	Nginx

Software Quality Attributes

Protectimus is developed in accordance with established software engineering practices to ensure reliability, maintainability, and performance.

The development process is based on the following principles:

- Use of standard libraries and proven development frameworks;
- Adherence to coding standards and best practices;
- DRY (Don’t Repeat Yourself) principles;
- Test-driven development (TDD).

Functional Capabilities

Protectimus provides a set of capabilities for managing authentication, enforcing security policies, and supporting user operations.

Authentication and Access Control

- Multi-factor authentication for users and administrators with configurable security policies per resource.
- Support for multiple authentication flows, including OTP-only authentication.
- Protection against brute-force attacks with limits for authentication attempts and automatic blocking.

Security Controls

- IP-based access restrictions.
- Geographic filtering.
- Time-based access policies.
- Transaction verification using Confirm What You See (CWYS).

Authentication Methods and Delivery

- Support for multiple OTP generation and delivery methods, including mobile apps, hardware tokens, push notifications, messaging platforms, SMS, and email.
- Flexible configuration of OTP parameters, including lifetime and length, with support for PIN protection.

Directory Integration and Advanced Authentication

- Integration with Active Directory, LDAP, and other user directories, including synchronization of users for centralized authentication management.
- Support for environments with multiple directory domains.
- Dynamic Strong Password Authentication (DSPA) is a directory-integrated authentication method that replaces static passwords with dynamic OTP credentials and supports OTP-only authentication.
- Support for passwordless authentication scenarios.

User Self-Service

- Self-service portal for users to manage authentication data and tokens.
- Token enrollment, replacement, and synchronization.
- Password management capabilities within administrator-defined policies.
- Administrator-controlled access to self-service functions.

Self-Service Password Reset (SSPR)

- Users can independently change and reset Active Directory passwords without administrator involvement.
- Password reset without old password (for recovery scenarios).
- Integration with multi-factor authentication for identity verification.
- Support for multiple authentication methods (AD credentials, Protectimus password, email OTP, security questions).
- Secure communication with Active Directory over LDAPS (SSL).
- Reduces IT workload and minimizes user downtime.

Administration and Monitoring

- Role-based access control for administrators with permissions scoped by resources and administrative roles.
- Event logging and audit capabilities.
- Reporting and analytics for authentication activities.

Solution Architecture

Architecture Overview

The solution is built using a modular service-oriented architecture, designed for scalability, reliability, and flexible integration with external systems.

The solution can be deployed either as a cloud service or as an on-premise platform within the customer's infrastructure. In both cases, Protectimus provides a centralized authentication system that processes authentication requests and enforces security policies.

The overall architecture of the platform is shown in Figure 1:

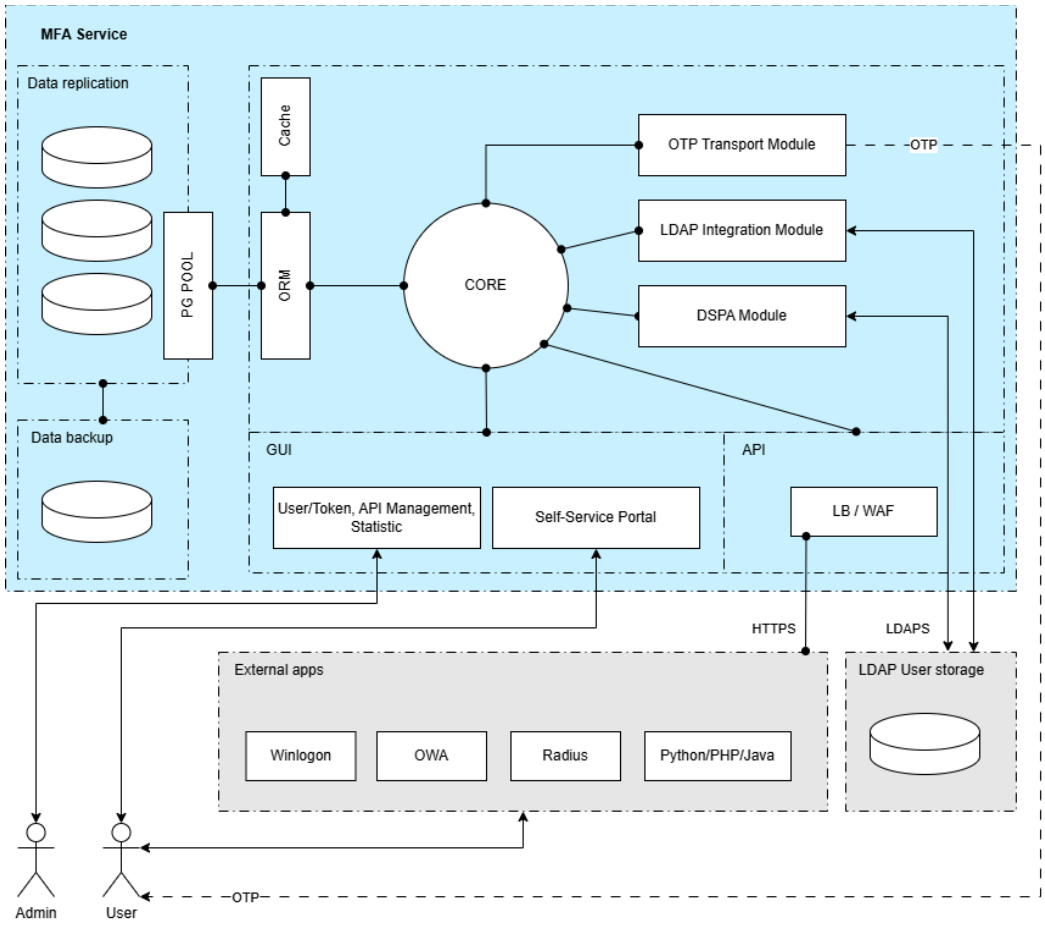


Figure 1. Overall Solution Architecture

Figure 1 illustrates the high-level architecture of the MFA service and the interaction between its core components, supporting services, and external systems.

To ensure reliable and continuous operation, the system is deployed in a cluster of high-performance servers:

- A Load Balancer distributes traffic across servers.
- A monitoring system continuously tracks the state of the infrastructure and notifies Protectimus administrators about potential threats and incidents.
- A Web Application Firewall (WAF) protects APIs from attacks. It acts as a filter between users and the service, analyzing HTTP/HTTPS traffic and blocking suspicious or malicious requests.

The **Core** component:

- processes authentication requests,
- enforces security policies,
- coordinates the operation of system components.

The **Core** is certified for compliance with OATH standards (HOTP, TOTP, OCRA).

User authentication processes are handled via a RESTful API (JSON/XML), which interacts with client systems such as Winlogon/RDP, OWA, RADIUS, VPN, and other applications.

GUI — a web interface for system configuration, user and token management, API configuration, and monitoring for administrators. It also provides users with extended self-service capabilities.

The data layer supports replication and backup, while sensitive data is protected by dedicated security components.

Infrastructure services such as caching, load balancing, WAF, and monitoring ensure performance, scalability, and reliability.

Key Modules

The solution architecture brings together several key modules that work in synergy to deliver a complete and robust authentication process.

- The **OTP Transport Module** is responsible for generating and delivering one-time passwords via mobile applications, hardware tokens, push notifications, messengers, SMS, and email, based on OATH standards (HOTP, TOTP, OCRA). SMS delivery via external providers is supported, including mechanisms based on SMTP.

- **LDAP Integration Module** — connects to external user directories (e.g., Active Directory or LDAP), enables user synchronization, and supports authentication scenarios based on defined parameters.
- **The Dynamic Strong Password Authentication (DSPA) module** integrates with external user directories such as Active Directory and LDAP, automatically replacing static user passwords with dynamic OTP-based credentials according to predefined policies and schedules.

Authentication Flow

Protectimus acts as a centralized authentication layer between protected systems and end users.

A typical authentication flow includes:

1. The user initiates access to a protected system or application.
2. The client system sends an authentication request to Protectimus.
3. If required, Protectimus verifies user data and credentials using external directories such as Active Directory or LDAP.
4. Protectimus requests the second authentication factor (OTP).
5. The user enters a one-time password (OTP).
6. The client system submits the OTP to Protectimus for verification.
7. Protectimus validates the OTP and returns the authentication result to the client system.
8. The client system then grants or denies access.

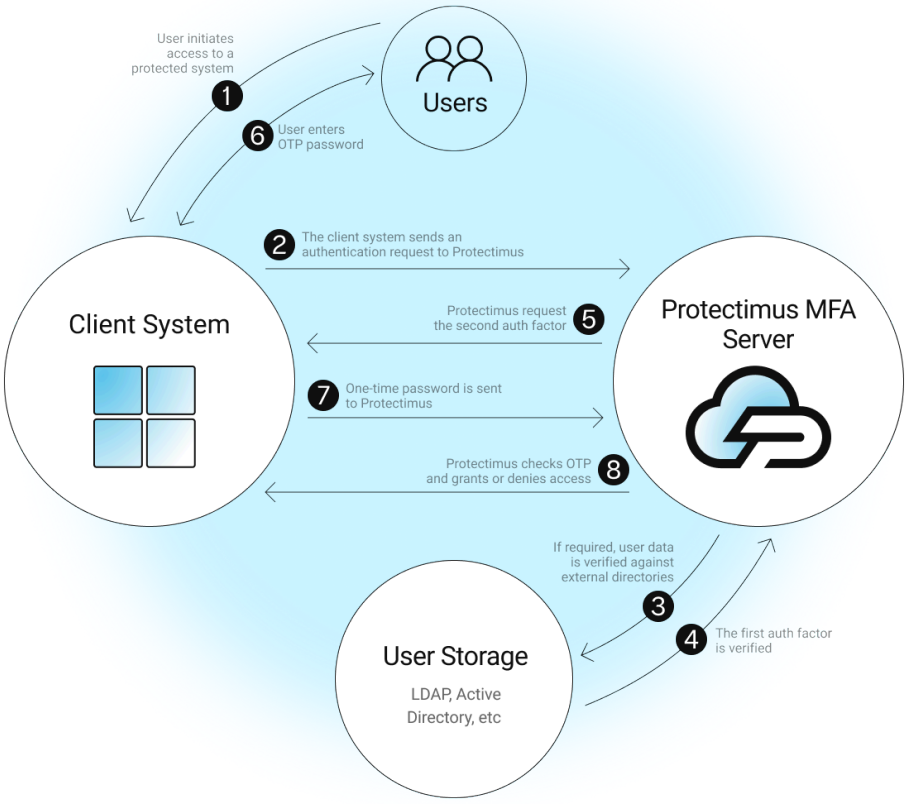


Figure 2. Typical authentication flow

Deployment Models

Protectimus supports two deployment models, allowing organizations to choose the approach that best fits their infrastructure and operational requirements.

- **Cloud-based (SaaS)** — a fully managed deployment operated by Protectimus, enabling rapid implementation without maintaining authentication infrastructure.
- **On-premise** — a self-hosted deployment within the customer's infrastructure, providing full control over data, configuration, and operations

On-premise deployments support both single-node installations and clustered multi-node configurations for scalability and fault tolerance.

High Availability and Data Protection

In on-premise environments, the system can be deployed in a cluster of high-performance servers. Load balancing distributes incoming traffic across nodes, while failover mechanisms ensure continuity in case of node failure. Monitoring components continuously track system health and generate alerts for administrators.

To prevent data loss and ensure recoverability, Protectimus uses a combination of regular backups and database replication.

Backups are stored on separate systems and provide multiple recovery points over time. Replication ensures that data changes are continuously synchronized across nodes, reducing the risk of data loss between backup intervals.

Together, these mechanisms ensure high availability, data integrity, and reliable system recovery.

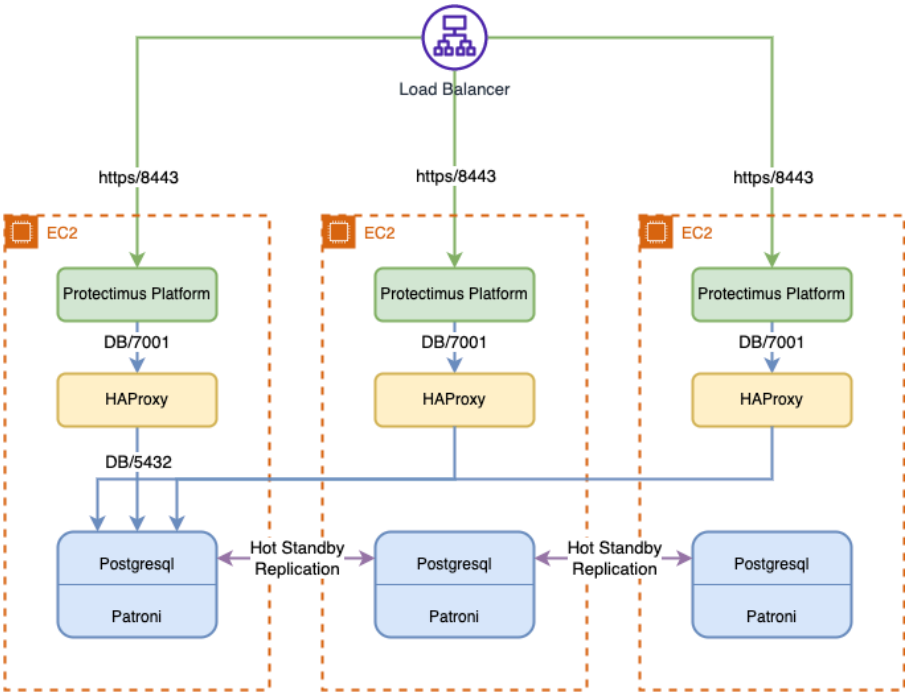


Figure 3. Cluster Architecture

Figure 3 illustrates a typical clustered deployment of the Protectimus platform in an on-premise environment.

The platform is deployed across multiple nodes to ensure high availability and fault tolerance. A minimum of three nodes is typically used to maintain cluster stability and quorum-based decision-making.

A load balancer distributes incoming requests across application nodes, ensuring efficient resource utilization and continuous service availability.

The database layer is deployed as a clustered system, where one node operates as the primary node responsible for processing write operations, while secondary nodes replicate data and can be used for read operations.

Cluster management and failover are handled by database clustering mechanisms, which monitor node health, perform automatic failover, and restore nodes after failure.

This architecture ensures continuous operation, minimizes downtime, and provides resilience against infrastructure failures.

Performance Optimization

Protectimus includes performance optimization mechanisms at multiple levels of the system architecture.

On the client side, optimizations include efficient resource handling and caching mechanisms.

On the server side, performance is enhanced through caching, optimized request processing, load balancing, and efficient handling of static content.

At the database level, performance is improved through optimized configurations and indexing.

Integration Approach

Protectimus integrates with external systems via a RESTful API, supporting data exchange in JSON and XML formats.

SDKs and client libraries are available for Java, Python, and PHP to support integration with custom applications.

The platform supports integration with enterprise systems, including VPNs, remote access solutions, web applications, and identity services.

Integration with Protectimus

Authentication Models

Protectimus enables multiple authentication models that can be applied depending on security requirements:

- **Password-based authentication.**
- **OTP-based authentication.**
- **Password + OTP (multi-factor authentication).**
- **OTP-only authentication (passwordless scenarios).**
- **Token-based authentication without user binding (resource-level validation).**

Authentication policies are configured per resource, allowing different rules for different systems and access scenarios.

Integration Methods

Protectimus can be integrated using multiple approaches depending on system architecture and requirements:

- **REST API integration** — the primary integration method, enabling authentication via API calls with support for JSON and XML formats. You'll find Protectimus API here.
- **SDKs and client libraries** — available for Java, Python, and PHP to simplify and accelerate integration.
- **Ready-to-use components and plugins** — for systems such as Windows Logon, RDP, ADFS, Outlook Web App (OWA), Roundcube, RADIUS-based solutions, VPNs, and web applications.
- **Embedded authentication (IFrame widget)** — for web-based authentication scenarios.

These options allow integration with both custom-built applications and enterprise systems.

Supported Integrations

Protectimus integrates seamlessly across endpoints, identity systems, infrastructure, and custom applications.

Endpoints & Systems

- **Windows Logon & RDP**
  Enables MFA for local and remote access to Windows systems
- **Linux & macOS**
  Enables MFA for non-Windows environments via RADIUS

Directories & Data Sources

- **Active Directory, LDAP, Databases**
  Enables directory-integrated authentication via DSPA, delivering MFA across multiple systems without client-side changes

Web & Identity

- **Microsoft ADFS**
  Enables MFA integration with federation services
- **Single Sign-On (SSO)**
  Allows secure access to enterprise applications via ADFS and Office 365

Network & Infrastructure

- **RADIUS-based Systems**
  Enables MFA for VPNs, Wi-Fi, firewalls, and other RADIUS-compatible systems

Email Systems

- **Outlook Web App (OWA) & EAC**
  Enables MFA for Microsoft Exchange web access
- **Roundcube**
  Enables MFA for webmail environments

Custom Integration

- **REST API (JSON/XML)**
  Enables direct integration with custom applications and services
- **SDKs (Java, Python, PHP)**
  Simplifies integration using client libraries

User Self-Service

Protectimus includes a self-service portal that can be integrated into authentication workflows, allowing users to manage authentication factors, enroll tokens, and perform secure password reset (SSPR) without administrator involvement.

Customization and Extensibility

Protectimus supports customization and extension to meet specific business and technical requirements:

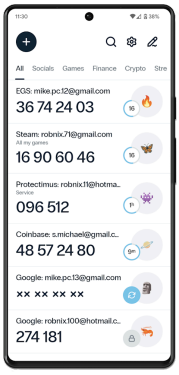
- Custom integrations and feature development.
- White-labeling of the platform, applications, and tokens.
- Adaptation to specific authentication flows and infrastructure.

This flexibility allows organizations to tailor the solution to their processes and security policies.

Authentication Methods and Tokens

Protectimus supports a wide range of authentication methods and token types, allowing organizations to choose the most suitable approach based on security requirements, user experience, and deployment scenarios.

Software Tokens



Protectimus Smart (mobile authenticator)
A free mobile authenticator app designed for secure and user-friendly authentication. Key features include encrypted cloud backup, seamless token transfer between devices, PIN and biometric protection, and support for push-based authentication and transaction verification (CWYS).

Push authentication
Fast and secure login confirmation via push notifications, reducing user friction while maintaining strong authentication security.

Hardware Tokens

Ideal for offline environments and high-security use cases.

Protectimus Slim NFC
Programmable TOTP token with NFC support, compatible with OATH-based MFA systems.

Protectimus Two
Hardware TOTP token with pre-configured secret keys and SHA-1 support.

Protectimus Flex
Programmable hardware TOTP token in a compact key fob format.

Protectimus Shark
Hardware TOTP token with pre-configured secret keys and SHA-256 support.

Out-of-Band Authentication

SMS-based OTP
One-time passwords are delivered via SMS through integration with external providers. In on-premise deployments, SMTP-based integration can be used for direct SMS gateway connectivity.

Email-based OTP
OTP delivery via email for user-friendly authentication scenarios.

Chatbot-based authentication
OTP delivery and confirmation via messaging platforms such as Telegram, Messenger, and Viber.

Advanced Authentication Methods

- **Confirm What You See (CWYS)**
  Transaction verification using contextual data to protect against phishing and man-in-the-middle attacks.
- **Passwordless authentication**
  Authentication using OTP-only flows without static passwords.
- **Directory-integrated authentication (DSPA)**
  Replaces static passwords with dynamic OTP credentials or enables OTP-only authentication within directory-based environments.

Graphical User Interface

Protectimus provides a web-based graphical user interface designed for efficient administration and intuitive system management.

The interface enables centralized control over users, tokens, resources, authentication policies, and system configuration.

Administrative operations such as token management, user configuration, and policy setup are optimized for speed and simplicity, minimizing operational overhead.

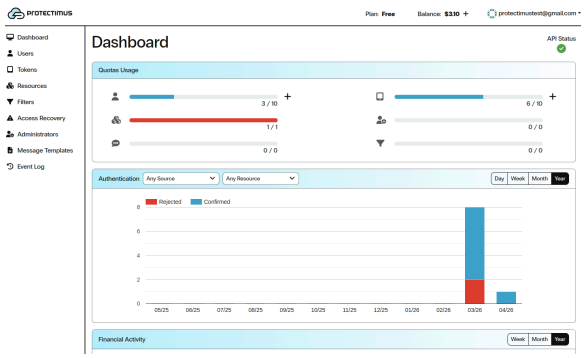
The interface supports dynamic updates and responsive interaction, ensuring real-time feedback and smooth system performance.

Monitoring and reporting tools, including authentication statistics and event logs, are available directly within the interface.

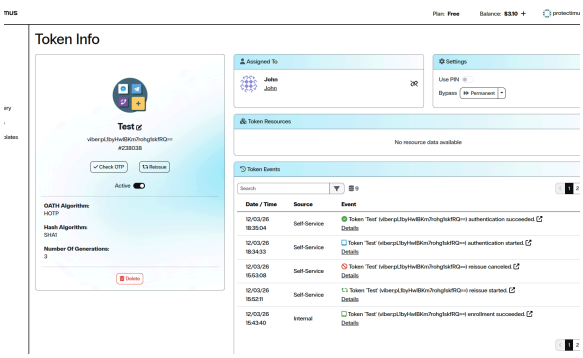
The user interface currently differs between the cloud-based service and the on-premise platform. These differences are temporary, with ongoing updates aimed at unifying the user experience across both deployment models.

SAAS Service Interface

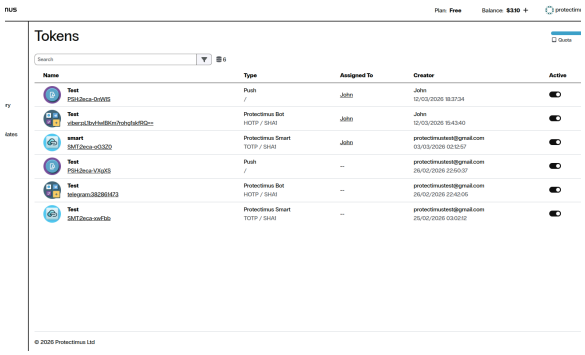
Control Panel



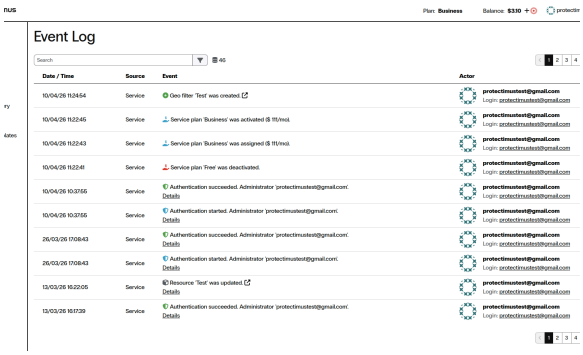
Editing Token Details



Tokens tab

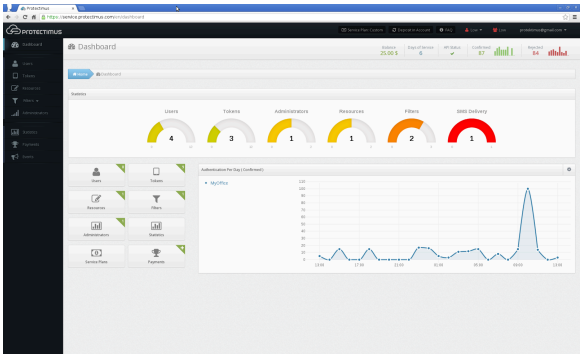


Event Log

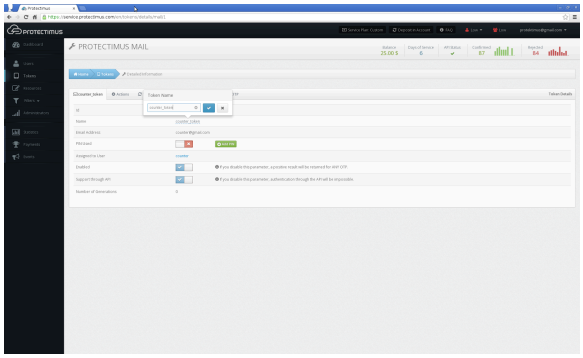


On-Premise Platform Interface

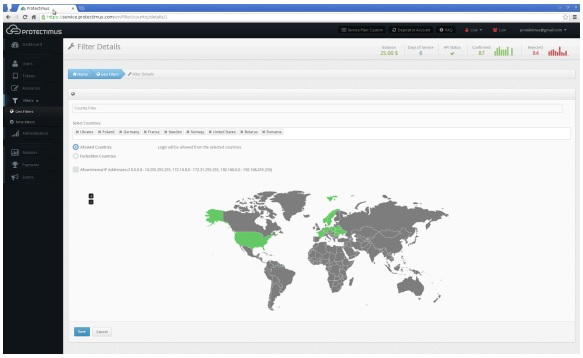
Control Panel



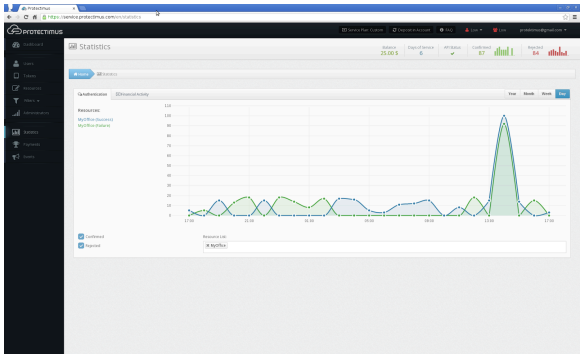
Editing Token Details



Geo Filters



Statistics



Contacts

Product issues, questions, or feedback
support@protectimus.com

Potential partnership discussion
sales@protectimus.com

Telephone Line
Ireland: +353 19 014 565
USA: +1 786 796 66 64

Corporate Details
Protectimus Ltd
Carrick House, 49
Fitzwilliam Square,
Dublin D02 N578,
Ireland