bamboocloud

Bamboocloud Next-Generation IAM

Product Whitepaper

Shenzhen Bamboocloud Technology Co., Ltd.

Headquarters address: 40F, Building A2, Creative City, Liuxian Avenue, Nanshan District, Shenzhen, Guangdong, China

Official website: en.bamboocloud.com

Telephone: 0755-86117880

Table of contents

1 Basic concepts

Access Control List (ACL)

An access control mechanism that manages and controls resource access by explicitly defining which users, groups, or devices can access specific resources and what operations (such as reading, modifying, or deleting) are permitted. ACL enables fine-grained control over resource management.

Single Sign-On (SSO)

An authentication mechanism that allows users to access multiple applications through a single login, without re-entering credentials for each application. Typically, SSO relies on a unified identity framework and standardized protocols, such as SAML, OAuth, or OIDC, to securely transfer authentication information across systems.

Multi-Factor Authentication (MFA)

A security enhancement over traditional password-based authentication systems, requiring users to provide two or more distinct types of credentials (such as a password, an SMS verification code, and a fingerprint) to verify their identity. By combining multiple authentication factors, MFA reduces the risk of single-factor compromise and mitigates threats such as account theft and data breaches.

Identity and Access Management (IAM)

A framework for managing user identities and controlling resource access. Its core functions include identity authentication, permission assignment, and access control, with the primary goal of ensuring that only authorized users can access specific systems or resources. In modern organizations,

IAM serves as a critical component for securing sensitive data and critical business systems.

Pluggable Authentication Module (PAM)

A flexible authentication mechanism that allows authentication methods to be configured without modifying the applications that utilize the authentication services. By modularizing the authentication process, PAM facilitates plug-and-play functionality for various authentication methods and enables easy addition, removal, or customization as needed.

Enterprise Application Integration (EAI)

A technical approach to connect independent application systems, data sources, and business processes within an organization to enable efficient data exchange and collaborative workflows.

In many enterprises, business systems are developed by different vendors and use diverse technical standards, thereby making direct inter-system communication difficult. EAI provides a unified integration platform where these isolated systems can work together cohesively and interconnectedly.

Role-Based Access Control (RBAC)

An access control mechanism that assigns permissions through roles. In RBAC, permissions are associated with specific roles, and administrators assign appropriate roles to users based on their job responsibilities or functions. These roles then determine which resources users can access and what operations they can perform. Compared to assigning permissions directly to individual users, RBAC simplifies permission management and improves efficiency.

2 Product overview

Digital identity forms the foundation for activities in the digital space and bridges the physical and virtual worlds. However, as digital transformation advances, identity governance becomes increasingly complex for enterprises. Issues such as identity theft and data breaches present significant security threats.

To address the security challenges posed by multi-dimensional identities in this interconnected era, Bamboocloud has independently developed a next-generation identity and access management (IAM) solution. The product is built on thorough analyses of user pain points and provides unified identity, access, and permission management services for modern organizations.

Identity management

The identity management service allows enterprises to centrally store the identity information of various types of users (including internal employees, suppliers, external personnel, and business partners) and unify account management across business systems.

The service enables automated lifecycle management of digital identities for users and applications through onboarding, internal transfers, position changes, and offboarding processes, preventing security risks associated with unauthorized accounts, dormant accounts, and accounts of former employees.

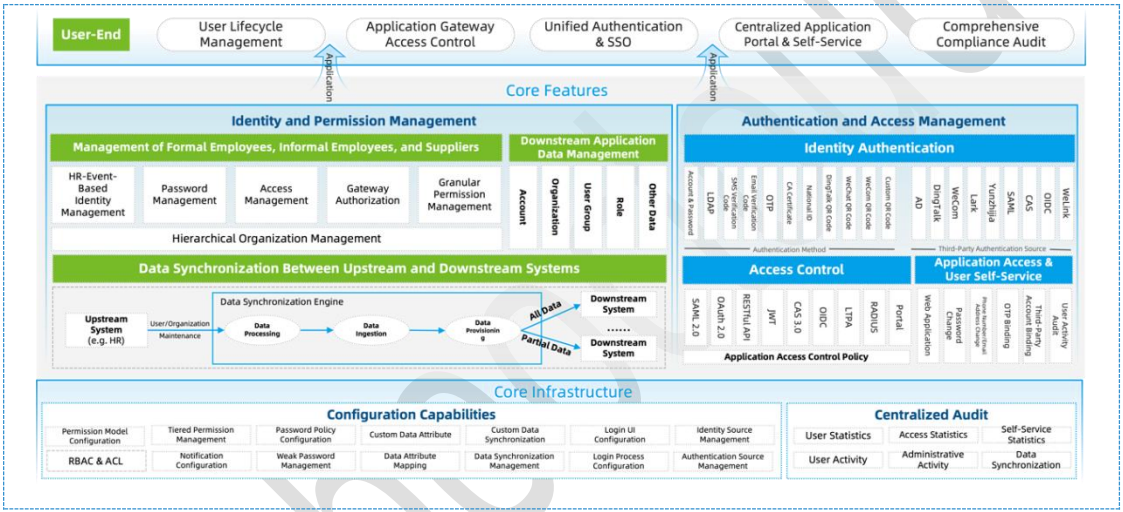
Access management

The access management service incorporates various authentication methods and allows flexible authentication combinations for multi-channel access across web, mobile, and desktop platforms, enhancing

both security and convenience of identity authentication.

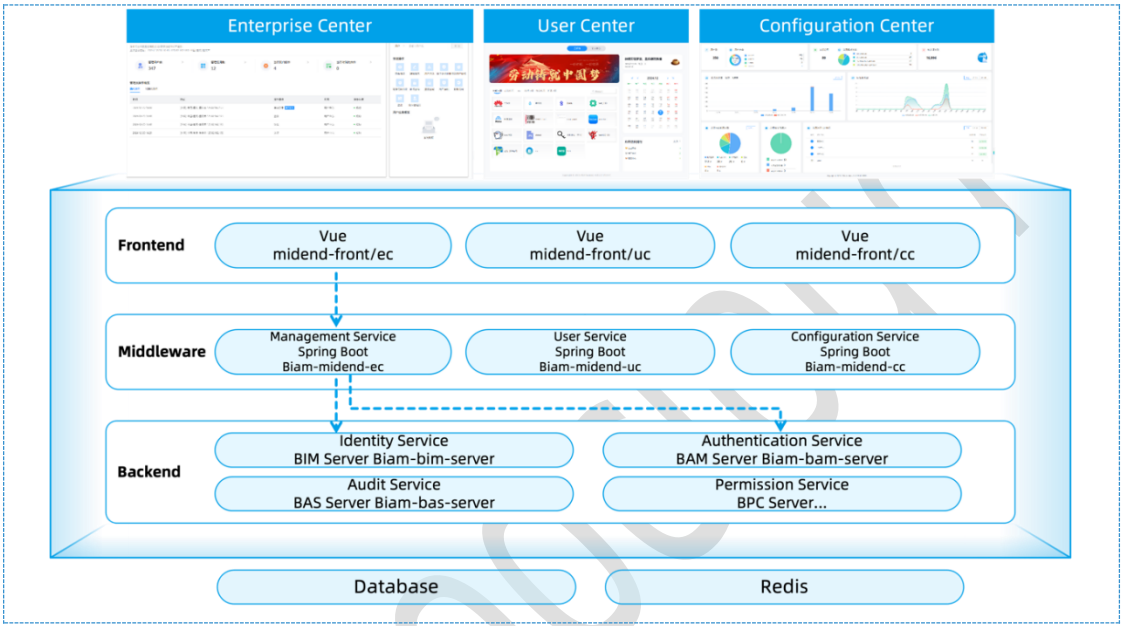
Permission management

The permission management service provides fine-grained permission management tools that simplify authorization workflows and enable centralized control over application permissions. It optimizes application system efficiency while ensuring secure and compliant permission management.



3 Product architecture

3. 1 System architecture



Bamboocloud IAM offers dedicated functional portals for different user roles to meet enterprises' multi-role and multi-scenario needs.

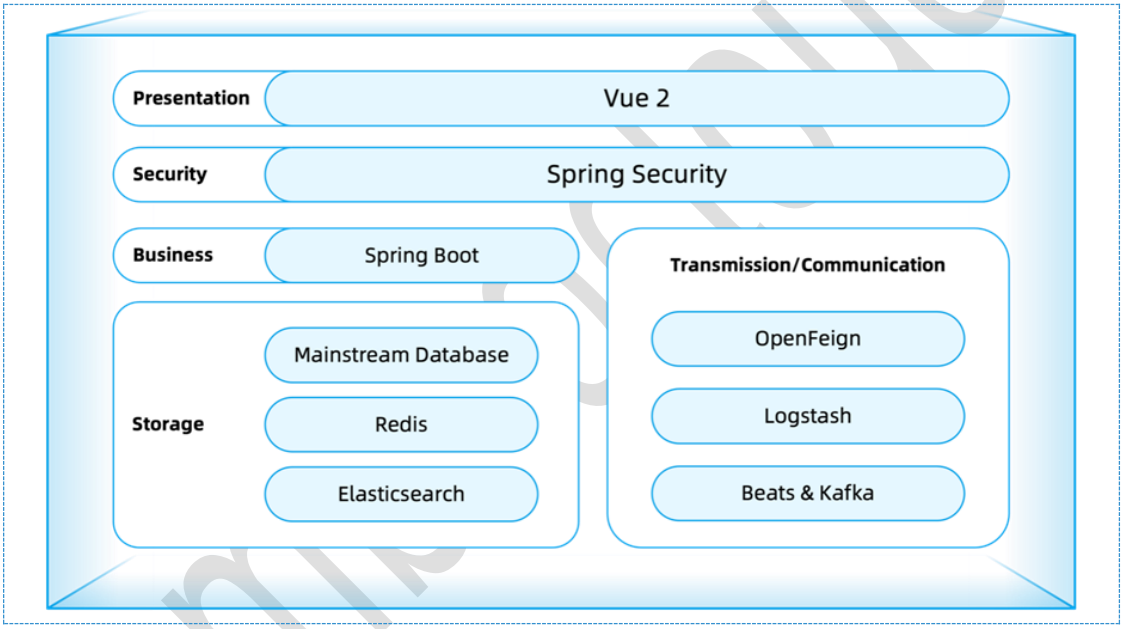
- **Enterprise center**: Serves enterprise-level identity administrators and application administrators, providing global identity and access management capabilities.
- **User center**: Serves internal employees and external personnel, providing a unified identity authentication and application access experience.
- **Configuration center**: Serves Bamboocloud IAM platform administrators, providing system configuration, monitoring, and operation and maintenance functionalities.

The overall system architecture consists of three tiers — frontend, middleware, and backend — ensuring flexible scalability and stable

operations through layered design.

- **Frontend**: Developed using the Vue framework, providing dedicated user interfaces for the enterprise, user, and configuration centers.
- **Middleware**: Built with Spring Boot to implement management, user, and configuration services, handling the business logic for each center.
- **Backend**: Offers core service components, including identity, authentication, audit, and permission services.

3. 2 Technology stack



Presentation layer

The presentation layer is built with the lightweight Vue 2 frontend framework to create an intuitive, responsive user interface with dynamic data interactions and seamless page switch. This enables a smooth user experience with minimal learning curves, achieving features such as real-time form validation and dynamic data visualization with instant updates.

Security layer

The security layer implements multi-level security protection using Spring Security, including unified identity authentication, granular permission

controls, and encrypted data transmission.

For instance, sensitive enterprise data is made accessible only to authorized personnel, thus preventing unauthorized access or data breaches while meeting compliance requirements in high-security scenarios for sectors such as finance and government.

Business layer

The business layer integrates the business logic and microservices architecture with Spring Boot, supporting rapid iteration and flexible scaling. New business modules (such as payment or approval) can be deployed independently with no system coupling, shortening the deployment cycle and adapting to diverse business requirements.

Storage layer

- **Redis 6.x.x**: A high-performance in-memory database that supports second-level responses for hot data queries, effectively handling high-concurrency scenarios and preventing system slowdowns.
- **Elasticsearch 7.x.x**: Provides full-text search and big data analytics capabilities for authentication log queries, operation log searches, and authentication behavior reporting.
- **Multi-database support**: Compatible with mainstream databases such as MySQL and Oracle, ensuring reliable and compatible data storage for enterprise-grade data management.

Transmission and communication layer

- **OpenFeign**: Simplifies remote service communication and improve system collaboration efficiency.
- **Logstash and Beats (Filebeat) 7.x.x**: Automates collection, cleansing, and aggregation of logs and metrics for quick system anomaly detection.
- **Kafka 3.x.x (Scala 2.13)**: Enables high-throughput message queuing

and support real-time data stream processing (such as user behavior analysis and IoT device data synchronization), ensuring system stability even during peak loads.

4 System requirements

4. 1 Infrastructure software compatibility

Item	Description
Server operating system	Mainstream operating systems, such as Kylin OS ARM/x86, NeoKylin ARM, UnionTech UOS x86, and CentOS x86. **Note**: Kylin OS ARM/x86 and CentOS x86 support automatic deployment.
Database	Mainstream databases, such as DM 8.1, KingbaseES v008R006C008B0014, GaussDB 3.223 Enterprise Edition, Vastbase G100_2.2, MySQL 8.0.x, and Oracle 19c. **Note**: MySQL 8.0.x supports automatic deployment.
Middleware	Mainstream middleware, such as TongWeb 7.0.4.7, Kingdee, and Tomcat 9.0.x. **Note**: Tomcat 9.0.x supports automatic deployment.

4. 2 Browser compatibility

4. 2. 1 User center and enterprise center

Compatible browsers and versions

Browser	Version
Microsoft Internet Explorer	10 and above
Microsoft Edge	98 and above
Google Chrome	80 and above
Mozilla Firefox	80 and above

Browser	Version
Safari	16.1
360 Extreme Browser	13.5 and above
360 Secure Browser	13.1 and above
Sogou Browser	11.0 and above
QQ Browser	11.0 and above
Cheetah Browser	6.5 and above

Recommended configuration

Item	Resolution	Zoom level
User center	At least 1920 × 1080	100% ~ 150%
Enterprise center	At least 1920 × 1080	100%

Note: The user center supports mobile access (including tablets) with a dedicated interface, which requires mainstream mobile browsers such as Edge 120+ for optimal performance.

4. 2. 2 Configuration center

Compatible browsers and versions

Browser	Version
Microsoft Edge	120 and above
Google Chrome	121 and above
Mozilla Firefox	122 and above
Safari	16.1
360 Extreme Browser	13.5 and above
360 Secure Browser	13.1 and above
Sogou Browser	11.0 and above
QQ Browser	11.0 and above
Cheetah Browser	6.5 and above

Recommended configuration

- Resolution: At least 1920 × 1080
- Zoom level: 100%

Note: The configuration center does not support access via Microsoft Internet Explorer.

4. 3 Resource requirements

4. 3. 1 Small-scale deployment

Scope

- User count ≤ 10,000
- Application count ≤ 50

Recommended Server Configuration

Type	Configuration	Quantity	Notes
Middleware server	• CPU: 16 cores • Memory: 32 GB • System disk: 120 GB SSD (RAID1)	2	-
Core server	• CPU: 16 cores • Memory: 32 GB • System disk: 120 GB SSD (RAID1)	2	-
Component server	• CPU: 16 cores • Memory: 64 GB • System disk: 120 GB SSD (RAID1) • Data disk: 240 GB SSD (RAID1)	3	-

Type	Configuration	Quantity	Notes
Backup and operations server	• CPU: 4 cores • Memory: 8 GB • System disk: 120 GB SSD (RAID1) • Data disk: 500 GB HDD (RAID1)	1	• Optional, deploy as needed. • The data disk must be a local HDD.
Total: 8 servers			

Note:

- System and data disks must use separate physical disks.
- Server capacity can be horizontally scaled to meet performance requirements in different business scenarios.

4. 3. 2 Medium-scale deployment

Scope

- 10,000 < User count ≤ 100,000
- Application count > 50

Recommended server configuration

Type	Configuration	Quantity	Notes
Middleware server	• CPU: 16 cores • Memory: 32 GB • System disk: 120 GB SSD (RAID1)	2	-
Core server	• CPU: 16 cores • Memory: 32 GB • System disk: 120 GB SSD (RAID1)	6	-

Type	Configuration	Quantity	Notes
Database server (for the access management service)	• CPU: 16 cores • Memory: 64 GB • System disk: 120 GB SSD (RAID1) • Data disk: 240 GB SSD (RAID1)	2	Physical servers are recommended.
Database server (for the identity management service)	• CPU: 16 cores • Memory: 64 GB • System disk: 120 GB SSD (RAID1) • Data disk: 240 GB SSD (RAID1)	2	Physical servers are recommended.
Database server (for the permission management service)	• CPU: 16 cores • Memory: 64 GB • System disk: 120 GB SSD (RAID1) • Data disk: 240 GB SSD (RAID1)	2	• Deploy only if the permission management service is needed. • Physical servers are recommended.
Component server	• CPU: 16 cores • Memory: 64 GB • System disk: 120 GB SSD (RAID1) • Data disk: 480 GB SSD (RAID1)	3	Physical servers are recommended.
Backup and operations server	• CPU: 4 cores • Memory: 16 GB • System disk: 120 GB SSD (RAID1)	1	• Optional, deploy as needed.

Type	Configuration	Quantity	Notes
	● Data disk: 1 TB HDD (RAID1)		● The data disk must be a local HDD.
Total: 18 servers			

Note:

- System and data disks must use separate physical disks.
- Server capacity can be horizontally scaled to meet performance requirements in different business scenarios.

4. 3. 3 Large-scale deployment

Scope

- User count > 100,000
- Application count > 50

Recommended server configuration

Type	Configuration	Quantity	Notes
Middleware server	● CPU: 16 cores ● Memory: 32 GB ● System disk: 120 GB SSD (RAID1)	3	-
Core server	● CPU: 16 cores ● Memory: 32 GB ● System disk: 120 GB SSD (RAID1)	9	-
Database server (for the access management service)	● CPU: 32 cores ● Memory: 64 GB ● System disk: 120 GB SSD (RAID1)	2	Physical servers are recommended.

Type	Configuration	Quantity	Notes
	● Data disk: 240 GB SSD (RAID1)		
Database server (for the identity management service)	● CPU: 32 cores ● Memory: 64 GB ● System disk: 120 GB SSD (RAID1) ● Data disk: 480 GB SSD (RAID1)	2	Physical servers are recommended.
Database server (for the identity management task handling)	● CPU: 32 cores ● Memory: 64 GB ● System disk: 120 GB SSD (RAID1) ● Data disk: 480 GB SSD (RAID1)	2	Physical servers are recommended.
Database server (for the permission management service)	● CPU: 32 cores ● Memory: 64 GB ● System disk: 120 GB SSD (RAID1) ● Data disk: 480 GB SSD (RAID1)	2	● Deploy only if the permission management service is needed. ● Physical servers are recommended.
Component server	● CPU: 32 cores ● Memory: 128 GB ● System disk: 120 GB SSD (RAID1) ● Data disk: 960 GB SSD (RAID1)	3	Physical servers are recommended.
Backup and operations server	● CPU: 4 cores ● Memory: 16 GB	1	● Optional, deploy as needed.

Type	Configuration	Quantity	Notes
	• System disk: 120 GB SSD (RAID1) • Data disk: 1 TB HDD (RAID1)		• The data disk must be a local HDD.
Total: 24 servers			

Note:

- System and data disks must use separate physical disks.
- Server capacity can be horizontally scaled to meet performance requirements in different business scenarios.

5 Core services

5. 1 Identity management

5. 1. 1 Background

With the continuous advancement of cloud computing, big data, IoT, and artificial intelligence technologies, traditional business models and processes are undergoing progressive digital and intelligent transformation. Enterprise applications are rapidly expanding to cover a broad range of business systems, including human resource (HR) management systems, collaborative office systems, financial management systems, and email systems.

Due to differences in implementation timelines, information security requirements, and construction standards, the organizational structures, user accounts, and access permissions across these systems often remain isolated and fragmented, resulting in the so-called "identity silos".

Moreover, as enterprise structures grow increasingly complex, the types of users within organizations also have diversified to include internal employees, temporary staff, external partners, suppliers, and more. Without a unified user management framework and identity governance mechanism, enterprises often encounter challenges such as inefficient operations and maintenance, heightened information security risks, and elevated management costs.

In today's sophisticated information security landscape, traditional measures are no longer sufficient to address emerging use cases. Strengthening internal controls and implementing continuous, dynamic management of both internal and external users has become a necessity for modern enterprises to protect core assets, reduce costs, and improve

operational efficiency.

5. 1. 2 Service objective

- Centralize digital identity management for enterprise users (including internal users, suppliers, external personnel, and business partners) and application systems.
- Implement automated and intelligent lifecycle management to address security issues caused by delays, inefficiencies, and human errors in manual operations.
- Mitigate security risks associated with unauthorized accounts, dormant accounts, and unrevoked accounts of former employees.
- Improve overall efficiency through precise, automated, and secure enterprise identity management to facilitate smooth business operations and streamlined workflows.

5. 1. 3 Service solution

With digital identity at its core, the identity management service helps enterprises establish a centralized and authoritative master data center. By providing unified standards and protocols for secure access to various application systems, the service enables automated management throughout the identity lifecycle, including onboarding, internal transfers, position changes, and offboarding.

In addition, the service offers distinct permission management views for administrators and individual users. Through data synchronization and custom connectors, it can integrate with various application systems to ensure automated synchronization of personnel data and application account information between the identity management system and integrated applications. This enhances overall enterprise operational efficiency and security.

5. 1. 4 Use scenarios

- **Growing number of enterprise users and applications**: As enterprises' digital transformation progresses, the number of internal applications and user types continues to grow, making identity and access management increasingly complex.
- **Decentralized account management**: Account operations such as creation, deletion, updates, and queries are handled by administrators for each application separately without a unified management process.
- **Time-consuming account provisioning**: Employee onboarding involving account and permission activation typically takes 3 to 5 business days, which severely hampers work efficiency.
- **Inconsistent password policies**: Applications enforce different password complexity rules without a unified standard, greatly increasing the difficulty of password management.
- **Resource inefficiency**: New business systems often require building separate user management frameworks from scratch when existing systems cannot be reused, resulting in wasted IT resources.
- **Lack of unified management standards**: The absence of unified standards for application account management and system integration further complicates administrative processes.

5. 1. 5 Core advantages

- **Tight business alignment**: Offer high flexibility, adaptability, and scalability to effectively meet the business requirements of real-world scenarios.
- **Comprehensive plugin support**: Compatible with plugins built via processors or scripts, which can be integrated at multiple extension points for customized functionality.
- **Effortless data migration**: Support importing and exporting business data, application configurations, and permission settings to improve

management efficiency.

- **Standardized interfaces**: Provide complete RESTful APIs to facilitate business process reengineering with features such as automatic data provisioning and synchronization, fully meeting the requirements of standardized integration.
- **Diverse interface types**: Offer a wide variety of commercial product connectors for plug-and-play integration with simplified configuration processes.
- **Customizable connectors**: Support flexible configuration of custom connectors for easy operations and streamlined development workflows.
- **Multi-layered data security**: Implement encrypted storage and display of sensitive data to ensure security during data storage and transmission.
- **Full identity lifecycle management**: Cover the entire identity lifecycle, including account creation, modification, and deletion.
- **Streamlined data synchronization**: Support synchronization of user identity data from authoritative identity data sources to ensure identity consistency across downstream systems.
- **Simplified password management**: Offer features such as automatic password generation, password policy validation, and encrypted password storage to enable secure and efficient password management.
- **Comprehensive audit**: Provide multi-dimensional audit reports for user authentication, access, and operations to help enterprises meet compliance requirements.
- **Granular permission management**: Support role-based permission management across multiple dimensions, including organizations, user groups, users, applications, and account types, for flexible and precise permission control.

5. 1. 6 Feature overview

Feature	Description
Management data dashboard and quick actions	● Display key management metrics, including the number of users and applications that can be managed within administrators' granted permissions. ● Display basic information about logged-in users, last login details, and audit operation records. ● Provide quick action buttons for user and application management tasks, such as user information update, password management, user status control, and application authorization.
Organization and user management	● Maintain user and organization information, control statuses, and perform import and export operations across multi-organization structures. ● Manage user account passwords and account lockout statuses. ● Assign application access or administrator privileges to users.
Application management	● Batch assign access to a single application to multiple users. ● Manage accounts, organizations, and groups for a single application.
Audit management	● Audit user authentication, application single sign-on (SSO) activities, and self-service operations in the user center, with visual bar charts to illustrate operational trends.

Feature	Description
	• Track management activities of platform administrators. • Provide user inventory statistics to assist administrators in gaining insights into overall user data, including the total user count, change trends, and distributions by user type, account status, and permission level. • Provide authentication statistics with distributions and rankings for a comprehensive overview of user authentication activities, including daily and monthly active user counts, authentication trends, times, methods, and statuses. • Provide self-service activity statistics with distributions and rankings to give administrators better visibility into self-service usage, including daily and monthly self-service user counts, operation trends, times, types, and results.
Platform management	• Implement role-based access control (RBAC) for platform permission management. • Support hierarchical data management for applications and organizations. • Visualize synchronization events generated during data synchronization for tracking and analyzing the synchronization process. • Support visualized management of third-party attributes for users and organizations to facilitate integration and maintenance of external data.

Feature	Description
	• Support user access and account status control, such as unlocking accounts and logging users out.

5. 2 Access management

5. 2. 1 Background

As enterprises accelerate their digital transformation, the variety and number of business systems continue to increase. Legacy systems that are difficult to replace often lead to growing maintenance and management needs, which further results in a significant amount of redundant and duplicated data. Additionally, high interdependency among these systems also complicates management and increases administrative workloads.

To improve management efficiency and maximize the reuse of existing systems, many organizations are adopting enterprise application integration (EAI).

EAI can be implemented at multiple levels, including data centralization at the data storage layer, universal data exchange at the data transmission layer, business process integration at the application layer, and the creation of a unified enterprise portal at the user interface layer. Among these, identity authentication integration (commonly referred to as SSO) is particularly critical.

In traditional enterprise IT environments, independent application systems typically have separate security frameworks and authentication mechanisms. This means that users must log in and out of each system they access individually, while authentication credentials remain system-specific and cannot be shared across systems. This not only escalates the complexity of system management but also introduces several security and operational challenges, including:

- **Authentication vulnerabilities**: Weak passwords or reliance on single-factor authentication are common in enterprises, making it easier for malicious actors to breach and gain unauthorized access to business systems.
- **Data security risks**: Without robust and reliable authentication mechanisms, sensitive and confidential enterprise data is more susceptible to theft or tampering.
- **Poor user experience**: Users have to remember multiple sets of credentials for different systems and repeatedly perform authentication and login, which significantly decreases productivity and degrades user experience.
- **High IT costs**: Maintaining separate authentication systems for each application requires substantial time, financial resources, and manpower to support the IT security infrastructure, thereby driving up overall operational costs.

5. 2. 2 Service objective

- Build a secure, unified, and innovative authentication platform for enterprises to meet diverse authentication needs.
- Provide various authentication methods and enable flexible authentication combinations for multi-channel access across web, mobile, and desktop platforms.
- Optimize resource allocation and operational efficiency while reducing IT maintenance burdens.

5. 2. 3 Service solution

Based on the pluggable authentication module (PAM) mechanism, the Bamboocloud access management service enables plug-and-play authentication, one-click integration, and unified authentication and access management for enterprise business systems.

The service provides authentication engine configuration (supporting both

biometric and non-biometric authentication methods) and delivers robust identity authentication capabilities through configurable templates, including multi-factor and multi-biometric authentication.

By unifying authentication, authorization, and access engagement while integrating strong identity authentication, session auditing, and centralized management, the service assists enterprises in building an integrated security framework.

To meet diverse enterprise security requirements, the service supports multi-factor authentication with convenient configurations. It enables tailored authentication combinations for different business scenarios, ensuring secure access for various applications with varying security levels and authentication factors. This resolves inconsistencies and security vulnerabilities in user identity management at both technical and administrative levels.

The service includes multiple built-in passwordless authentication methods, such as mobile one-time passwords (OTPs), digital certificates, SMS verification codes, and dynamic tokens. Additionally, it supports standard authentication protocols such as SAML and OAuth, significantly enhancing identity authentication security to meet the demands of modern security frameworks.

5.2.4 Use scenarios

- **Fragmented authentication management**: The use of varying authentication methods across enterprise business systems, coupled with distinct management interfaces built by different vendors, significantly increases management complexity.
- **Inconsistent authentication interfaces**: The absence of unified standards for authentication interfaces necessitates separate development to meet the authentication needs of each application, leading to high development costs and challenging interface

maintenance.

- **Siloed authentication frameworks**: Independent authentication systems often fail to swiftly meet enterprise demands for diverse authentication scenarios.
- **Barriers in authentication channels**: Despite the widespread use of smartphones and mobile office solutions, integration between mobile and desktop authentication channels remains incomplete, impacting user experience and collaboration efficiency.
- **Diverse authentication scenarios**: Enterprises need to address authentication needs across various channels, including mobile applications, web applications, client/server applications, operating systems, IoT devices, and cloud platforms.
- **Complex authentication configuration**: Implementing multi-factor authentication solutions within enterprise systems requires rapid and straightforward configuration to ensure efficiency and usability.

5. 2. 5 Core advantages

- **Comprehensive application permission and access control configuration**: Enhance overall enterprise information security, strengthen privacy protection, and reduce security risks such as data breaches.
- **Unified access control framework**: Optimize resource allocation, lower development and maintenance costs, and increase overall operational efficiency.
- **Enhanced user experience**: Users only need to log in once to access all authorized application systems, avoiding repetitive logins and improving user convenience.
- **Efficient integration capabilities**: Support multiple integration methods (such as SDKs and RESTful APIs) to enable standalone authentication services and ensure non-intrusive, rapid integration with application systems.
- **Flexible multi-authentication**: Build an integrated authentication

framework and achieve plug-and-play functionality with the PAM mechanism, meeting the authentication needs of various channels (such as desktop applications, mobile applications, operating systems, IoT devices, and web applications).

- **Multi-layer security protection**: Support various access control methods, fine-grained authorization, authentication policy configurations, and authentication-chain-based step-up authentication to safeguard critical data and business systems.
- **Comprehensive security audit**: Provide thorough identity audit services, full-scenario logging of login and operation activities, and visualized reports, offering data insights for routine maintenance and security incident management.

5. 2. 6 Feature overview

Feature	Description
Authentication method	• Support password-based authentication via local databases, the LDAP protocol, and Microsoft Active Directory (AD). • Support authentication via SMS or email verification codes. • Support QR code-based authentication via DingTalk, WeCom, WeChat, Lark, and custom application systems. • Support OTP authentication via Google Authenticator, Microsoft Authenticator, or SDK-integrated mobile apps. • Support customizing and extending authentication methods as needed.
Application authentication integration	Support SSO integration through RESTful APIs and various authentication protocols, including LTPA, CAS, SAML, RADIUS, JWT, OIDC, OAuth, and Portal.

Feature	Description
Third-party authentication source	● Support application SSO via DingTalk, WeCom, Lark, and Cloud Hub workspaces. ● Support desktop SSO via the AD Kerberos protocol. ● Support application SSO upon authentication via SAML, CAS, and OIDC protocols. ● Support step-up authentication as configured in the authentication chain after initial third-party authentication.
Mobile integration	● Support authentication via passwords and SMS verification codes. Additional authentication for binding new devices can also be performed through SMS. ● Support OTP binding: Users can scan the QR code using a custom app and enter the app-generated OTP to complete the binding process. ● Support OTP generation: Users can view dynamic OTP codes and their expiration times on a custom app. ● Support QR code-based authentication: Users can scan the QR code on the desktop login page using a custom app for authentication. ● Support app list display: Users can browse the list of available applications on a custom app and access other mobile apps with one-click SSO. ● Support SSO: Users can access other mobile apps through the app list displayed on a custom app. If the target application is already integrated with the desktop authentication

Feature	Description
	system, no mobile-specific integration is required. ● Support device management: Users can view the list of bound devices and unbind devices using a custom app.
User self-service	● Support both desktop and mobile access with responsive interfaces. ● Display authorized applications and support password-free login with one-click SSO. When accessing applications configured with specific access control policies, users will be prompted to perform step-up authentication. ● Display personal information with sensitive data masked as needed. ● Users can change their password, phone number, and email address after authenticating via password, SMS, or email code. ● Provide personal activity statistics and audit logs. ● Support self-service OTP binding.

5.3 Permission management

5.3.1 Background

Modern organizations typically have a variety of application systems to manage their business, operations, and infrastructure. However, due to differences in implementation timelines, information security requirements, and construction standards—as well as the presence of numerous third-party applications—permission management frameworks vary across systems. This further leads to complicated permission management, decentralized management entry points, and reduced

operational efficiency.

Additionally, technical personnel are burdened with repetitive authorization tasks, resulting in both inefficiencies and low employee satisfaction. Therefore, it is necessary for enterprises to build a unified platform to standardize permission management across all business systems.

5. 3. 2 Service object

- Provide enterprises with an integrated permission management solution that simplifies authorization, strengthens control, and standardizes governance.
- Solve issues related to efficiency, user experience, and security across business systems.
- Achieve efficient, intelligent, and compliant permission allocation to ensure seamless collaboration and optimized workflows.

5. 3. 3 Service solution

The permission management service helps enterprises address key challenges in permission provisioning, querying, revocation, and overall management. It effectively mitigates associated security risks while improving operational efficiency, user experience, and cost-effectiveness through centralized management.

Furthermore, by providing enterprise-wide permission lifecycle management, the service establishes permission management mechanisms and creates an integrated solution ecosystem that unifies identity, access, and permission management alongside other services.

5. 3. 4 Use scenarios

- **Decentralized permission request process**: Multiple permission request channels and complex workflows result in lengthy approval

cycles and reduced operational efficiency.

- **Unclear permission definitions**: Excessive use of technical terminology in permission definitions makes them difficult to understand, increasing the costs of usage and management.
- **Lack of a unified permission model**: Inconsistent permission models across applications hinder the implementation of effective permission review and audit mechanisms.

5. 3. 5 Core advantages

- **Support for industry-standard permission models**: Compatible with widely adopted RBAC and access control list (ACL) models, along with role- and function-based permission definitions and authorizations, to meet the permission requirements of most application systems.
- **Dynamic permission model configuration for enhanced management**: Enable customized permission models and attribute settings for each application system. Administrators can monitor and manage the authorization workflow of all systems in real time, which optimizes multi-system maintenance efficiency.
- **Automated permission control for business security**: Support self-service permission requests, addressing challenges like single-system design limitations, high development workload, and lengthy deployment cycles; support automatic authorization upon approval, where account creation, modification, and one-click revocation are automatically performed once the approval process is completed; reduces delays and human errors by automating processes while maintaining comprehensive audit trails through approval records and authorization logs.

5. 3. 6 Feature overview

Feature	Description
Centralized permission management	• Support RBAC and ACL permission models.

Feature	Description
	● Support custom permission attributes. ● Support authorization based on users, accounts, roles, and functions.
User permission portal	● Support self-service permission requests. ● Support viewing existing permissions. ● Support tracking permission request status. ● Provide tailored permission request interfaces for different permission models.
Permission revocation and synchronization	Provide standard APIs for integration with various downstream systems to synchronize permissions, roles, and related mapping data.

6 Abbreviations

ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CAS	Central Authentication Service
EAI	Enterprise Application Integration
IAM	Identity and Access Management
IoT	Internet of Things
IT	Information Technology
JWT	JSON Web Token
LDAP	Lightweight Directory Access Protocol
LTPA	Lightweight Third-Party Authentication
MFA	Multi-Factor Authentication
OAuth	Open Authentication
OIDC	OpenID Connect
OTP	One-Time Password
PAM	Pluggable Authentication Module
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control
SAML	Security Assertion Markup Language
SDK	Software Development Kit
SSO	Single Sign-On