bamboocloud

Bamboocloud IDaaS

Product Whitepaper

Trademark

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

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.

Identity as a Service (IDaaS)

A cloud-based identity and access management solution providing user identity lifecycle management, unified authentication, single sign-on, and access governance as a service. It enables organizations to obtain

professional, scalable identity security capabilities without building complex identity infrastructure.

Software as a Service (SaaS)

A software delivery model where applications are hosted in cloud servers and delivered to users via the internet. Users can subscribe on-demand without maintaining the software themselves.

Security Assertion Markup Language (SAML)

An XML-based open standard data format for exchanging authentication and authorization data between security domains, where two key roles are defined: identity provider (IdP), which authenticates users, and service provider (SP), which grants access to applications or services.

Open Authorization (OAuth)

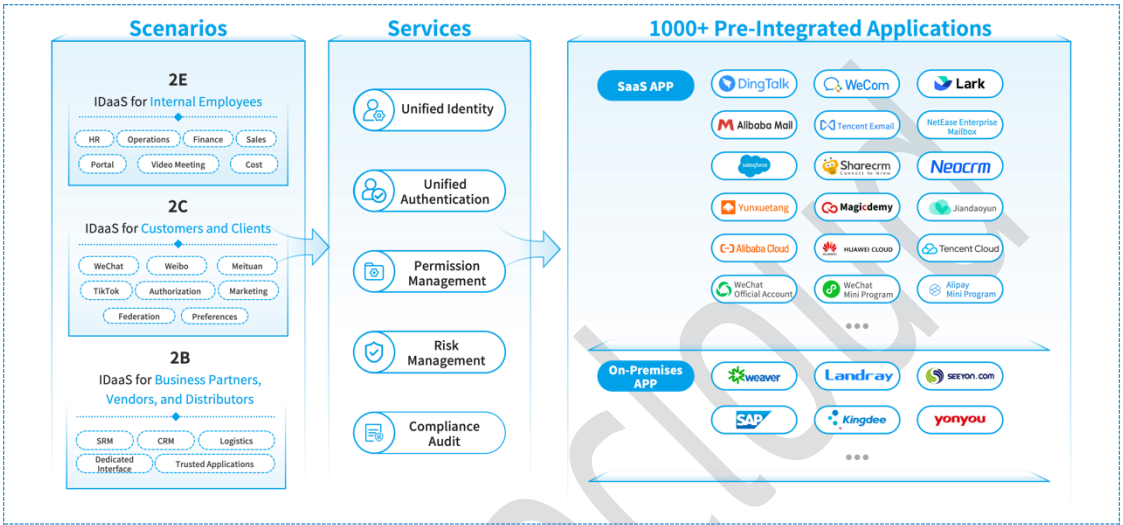
An open authorization protocol that enables users to grant third-party applications access to their data stored with other service providers without sharing credentials.

System for Cross-domain Identity Management (SCIM)

An open standard protocol designed to simplify user identity data synchronization, primarily used for data exchange between enterprise identity management systems and third-party applications.

2 Product introduction

2. 1 Product overview



As enterprises experience rapid business growth and undergo accelerated digital transformation, cybersecurity has become a central focus in enterprise management. Identity security, as a fundamental component of cybersecurity, serves not only as the cornerstone for security transformation but also as a critical pillar for building digital ecosystems, driving business innovation, and ensuring sustainable development.

However, with the increasing number of self-built enterprise applications and the widespread adoption of cloud computing and SaaS services, traditional identity management systems can no longer meet the diverse and complex identity security needs of modern organizations.

In this context, Bamboocloud IDaaS (hereafter IDaaS) has been developed as a cloud-based identity security product that focuses on comprehensive identity and access management (IAM) solutions across all scenarios, helping organizations establish a unified and secure identity management platform.

At the management level, IDaaS centralizes access control over all application resources based on user identities. At the user level, through the OneID mechanism, users can access all authorized applications with a single identity, significantly enhancing both security and access convenience.

With extensive technological expertise and implementation practices, IDaaS has pre-integrated with over 1000 domestic and international commercial applications including enterprise collaboration tools, email services, office solutions, financial systems, development platforms, cloud provider consoles, and social applications such as WeChat and Alipay. This enables enterprises to achieve quick business system integration with reduced development costs.

By offering unified identity, unified authentication, permission management, risk management, and compliance audit services, IDaaS comprehensively addresses the identity security needs of diverse user groups, including internal employees, business partners, suppliers, distributors, and customers.

Meanwhile, it enables efficient identity and access management across multiple channels such as web applications, mobile applications, mini-programs, official accounts, and internal business systems.

Unified identity

IDaaS helps enterprises build a comprehensive identity lifecycle management system that unifies identity data across business systems and ensures full consistency between online and offline identity frameworks. By addressing traditional isolated identity management issues, IDaaS mitigates security risks posted by orphan accounts, dormant accounts, and unauthorized accounts.

Unified authentication

IDaaS supports various authentication methods that enterprises can quickly configure to adapt to different scenarios. Users need to authenticate only once to access all business systems available to them.

Permission management

IDaaS supports automatic authorization based on multiple dimensions such as the organizational structure, user groups, positions, and user attributes, enabling centralized and fine-grained permission management for all business systems.

Risk management

IDaaS provides real-time intelligent risk alerts and controls based on factors such as operation scenarios, behavior patterns, user activities, and access environments to identify and mitigate potential identity fraud and account theft risks.

Compliance audit

IDaaS offers multi-dimensional audit reports that cover user authentication, access, and activities to help enterprises meet compliance requirements.

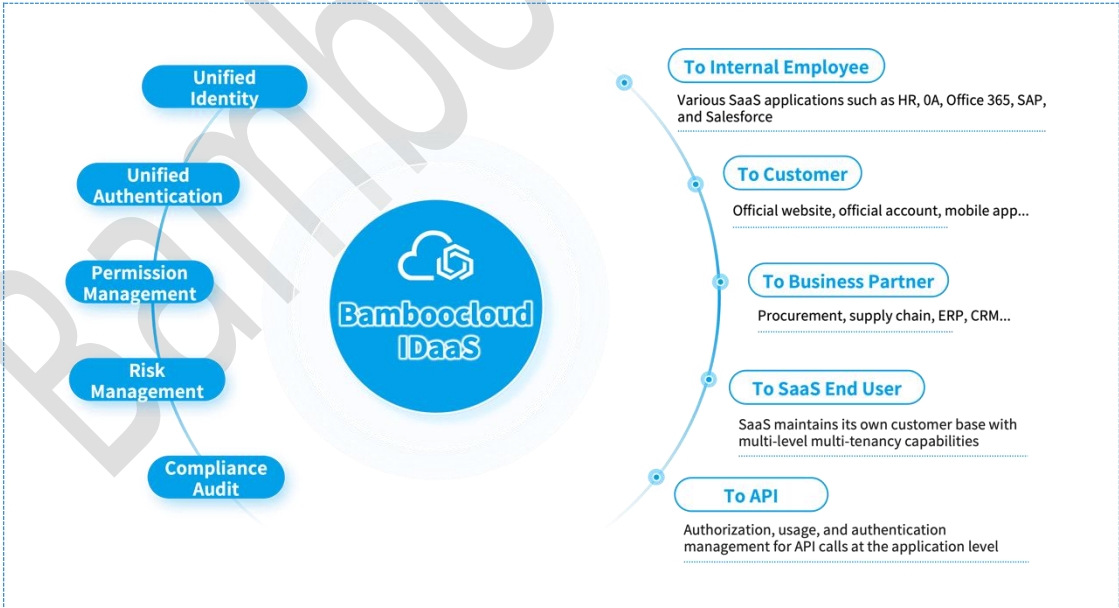
2. 2 Use scenarios

Based on different user types and application types, IDaaS can be applied to various business scenarios, fully meeting the identity security requirements of user groups including internal employees, business partners, suppliers, distributors, and customers.

User	Application	Scenario
Employee	Office and business applications	

User	Application	Scenario
Business partner	Supply chain and partner collaboration applications, such as bidding and procurement platforms, and agent management systems	Enterprise identity and access management (EIAM)
Customer	Official websites, mini-programs, official accounts, and various customer applications	Customer identity and access management (CIAM)

Beyond the above scenarios, IDaaS also supports authentication and authorization management for special resources such as application-level API calls.



2. 3 Core values

Enhanced digital management to drive operational excellence

- Establish unified standards, specifications, and interfaces
- Reduce digital transformation costs and redundant development expenses while providing robust support for efficient operations

Improved user experience and business collaboration

- Enable more efficient, convenient, and secure access to digital assets for internal users
- Enhance external user collaboration and experience while improving business process efficiency

Rapid organizational adaptability to support business expansion, merger, and acquisition

- Enable cross-regional, cross-platform, and cross-system business integration and resource coordination
- Support quick adaptation to organizational changes while facilitating digital transformation and refined management

Strengthened internal controls and regulatory compliance

- Implement unified, centralized identity cloud services to enhance the protection of enterprise digital assets
- Reduce data breach risks and meet regulatory compliance requirements

2. 4 Core advantages

Comprehensive: rich customer cases and extensive application ecosystem

IDaaS has successfully served over 2500 renowned enterprises globally with widespread adoption across various industries and use cases. The

platform comes with extensive pre-integrated applications that enable enterprises to achieve rapid integration and efficient deployment in minimal time without high costs.

Fast: efficient delivery and rapid implementation

With deep technical expertise and extensive project experience in IAM, IDaaS features a user-centric architecture and provides robust standardization capabilities that adapt flexibly to diverse business scenarios. The professional implementation team consists of seasoned IAM technical and business experts, ensuring efficient project implementation and rapid delivery.

Reliable: superior product quality and professional service

IDaaS has been battle-tested in over 2500 projects and earned user satisfaction through its high security, high availability, and high performance. The platform is supported by experienced implementation and after-sales teams providing 24/7 technical support, which continuously ensures stable operations and optimal user experience.

Cost-effective: optimizing resources for more focus on core business

Through automated processes, a pay-as-you-go cloud service delivery model, and out-of-the-box functionalities, IDaaS helps enterprises reduce hardware investments and maintenance costs while improving operational efficiency.

By optimizing resource allocation, enterprises can redirect more budgets toward innovation, research and development, and business expansion to enhance competitiveness and drive high-quality business development.

2. 5 Customer cases

Through its strong research and development innovation, professional

services, extensive implementation experience, and mature standardized integration capabilities, IDaaS has provided enterprise-grade digital identity security services to over 2500 renowned companies worldwide and more than 40 million users across scenarios involving employees, business partners, and customers.

The IDaaS team delivers comprehensive professional services throughout the entire lifecycle, from product consulting and solution design to project implementation, addressing identity and access management needs for customers in various industries such as energy, manufacturing, pharmaceutical, real estate, retail, and technology.

2. 6 Product qualifications and intellectual properties

With innovation as its core driving force, continuous investment in research and development of cutting-edge technologies, and strict adherence to industry standards, Bamboocloud has obtained multiple authoritative certifications and intellectual property achievements both domestically and internationally.

International standard certification

- ISO9001 Quality Management System
- ISO20000 Information Technology Service Management System
- ISO27001 Information Security Management System
- ISO27701 Privacy Information Management System
- ISO27018 Protection of Personally Identifiable Information in Public Clouds

Information security qualification

- Classified Protection of Cybersecurity Level 3 Certificate
- Information System Security Integration Service Qualification Level 2 Certificate Issued by China Cybersecurity Review Technology and Certification Center (CCRC)
- EAL3 Certificate Issued by China Information Technology Security Evaluation Center (CNITSEC)
- Computer Information System Security Product Sales License
- CS2 System Integration Qualification Certificate
- Information Technology Service Standard (ITSS) Operations and Maintenance Level 3 Certificate

Enterprise qualification

- Capability Maturity Model Integration (CMMI) Level 5 Certificate
- National High-Tech Enterprise Certificate
- Shenzhen Software Product Evaluation and Software Enterprise Evaluation Certificate
- Commercial Cryptographic Product Manufacturing Designated Enterprise
- Commercial Cryptographic Product Sales License
- AAA-Level Enterprise Credit Evaluation Certificate

Intellectual property and independent innovation

- Intellectual Property Management System Certificate

- 120+ Software copyrights
- 100+ Invention patents

3 Technical overview

3. 1 System architecture

IDaaS is a multi-tenant SaaS application built on cloud-native technologies, offering high availability, high scalability, high flexibility, and continuous integration capabilities.

Cloud-native infrastructure

Built on Kubernetes container services, IDaaS features a highly automated microservices architecture that allows dynamic orchestration and service management for flexible deployment of all microservices.

Meanwhile, IDaaS can perform real-time horizontal scaling based on workload demands, ensuring efficient and stable service delivery and meeting performance needs in large-scale data processing and high-concurrency business scenarios.

Highly available data storage

IDaaS implements a high-availability cluster deployment using cloud-native RDS databases with multi-replica backups, primary-secondary configurations, Elasticsearch for full-text search, and Kafka for message queuing to achieve reliable data storage.

This architecture ensures uninterrupted services through seamless failover mechanisms even during single points of failure, significantly enhancing system availability and disaster recovery capabilities.

Automated deployment and continuous delivery

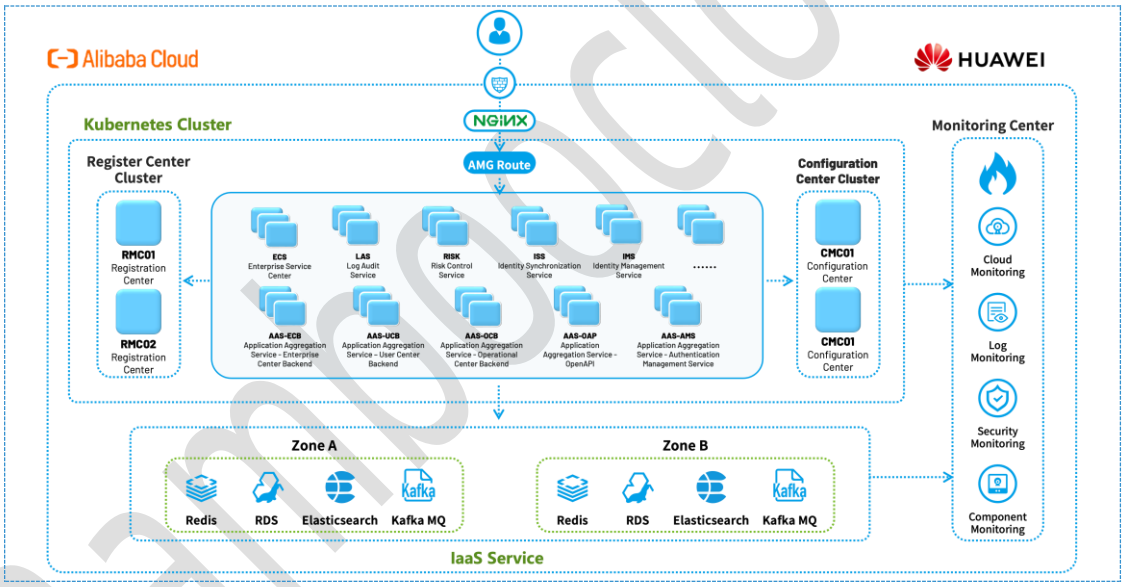
IDaaS supports automated CI/CD pipelines, uses blue-green deployment mechanisms for system upgrades, and allows flexible traffic routing based

on tenant-specific domain names.

During rapid version iterations, IDaaS ensures zero-downtime deployment of identity authentication services and meets enterprises' stringent requirements for business continuity.

Comprehensive monitoring and alerting

IDaaS provides real-time monitoring and alerting for all services and components. By collecting system performance metrics, log data, and anomaly events, it quickly identifies potential issues and triggers alerts. This ensures prompt response from operations teams and maintains high availability, stability, and security of the IDaaS platform.



3. 2 Integration solution

IDaaS provides a unified identity service that empowers enterprises to build a highly secure, scalable identity management system through robust integration capabilities and automated identity synchronization.

Designed to address the needs of diverse scenarios, the integration solution of IDaaS consists of three main components: identity source, authentication method, and business system.

Identity source integration

IDaaS comes pre-integrated with mainstream human resource (HR) systems as the upstream identity source, allowing quick integration through simple configuration without code modifications.

For HR systems not yet pre-integrated, efficient identity data synchronization can also be achieved through the platform’s standardized identity management APIs, ensuring consistent identity data across upstream identity sources and downstream business systems.

Authentication method integration

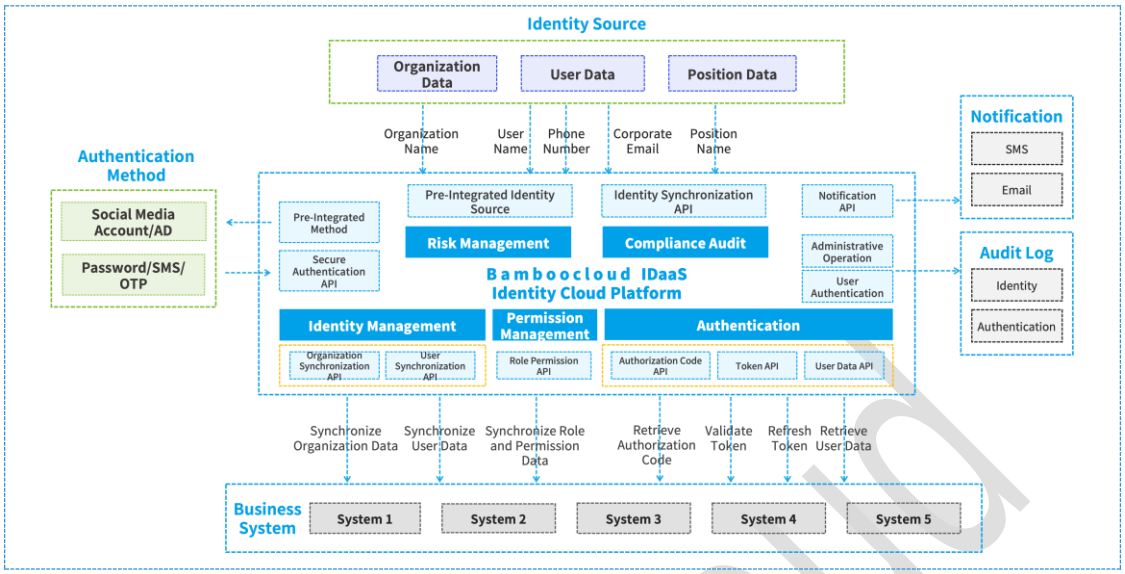
IDaaS supports multiple authentication methods, including account password, verification code, Fast Identity Online (FIDO) biometric authentication, and pre-integrated mainstream third-party authentication sources such as WeChat, Alipay, DingTalk, WeCom, and Lark.

Additionally, IDaaS allows authentication requests to be transferred to enterprises' on-premises authentication systems. If enterprises choose not to use the platform's unified login interface, they can implement seamless integration between business systems and IDaaS through secure authentication APIs to meet diverse authentication requirements.

Business system integration

IDaaS has pre-integrated with over 1000 common commercial applications, significantly reducing the time and resource costs of integration and development.

For enterprises’ self-developed business systems, IDaaS provides identity and authentication APIs compatible with international standard protocols, accompanied by detailed interface guides. This enables enterprises to quickly implement identity and authentication services, improving both integration efficiency and development experience.



3. 3 Security solution

As a cloud-based, multi-tenant SaaS identity platform, IDaaS implements comprehensive security measures across network transmission, runtime environment, data storage, and administrative operations to ensure the security and compliance of enterprise identity data. With authoritative security certifications (see the Product qualifications and intellectual properties section) obtained over the years, IDaaS provides enterprises with reliable identity security solutions.

Network transmission security

All platform pages and APIs utilize the HTTPS protocol based on TLS encryption, effectively preventing unauthorized access, data theft, and attacks while ensuring data integrity and confidentiality during transmission.

Runtime environment security

The IDaaS platform's runtime environment is fully protected by the cloud security center provided by the cloud service provider. Multi-layered security services, including web application firewall (WAF), cloud monitoring, real-time vulnerability scanning, and distributed denial-of-

service (DDoS) attack prevention, provide robust risk mitigation capabilities and ensure stable platform operation.

Data storage security

User passwords are stored using the bcrypt encryption algorithm with salted hashing to ensure irreversibility and prevent brute-force attacks. Sensitive user data (such as phone numbers and email addresses) is stored using symmetric encryption and displayed in masked formats (such as asterisks) in the enterprise management console to maximize user privacy protection.

Administrative operation security

During daily maintenance and management, strict access control is enforced through bastion hosts for all resource access. All administrative operations are logged and recorded for periodic reviews by compliance auditors, meeting enterprise requirements for data compliance and operational auditing.

4 Core services

4. 1 Unified identity

IDaaS provides a unified identity service for enterprises to centrally manage the digital identities of users and business systems. The service enables automated and intelligent lifecycle management for employee onboarding, position changes, internal transfers, and offboarding, significantly improving management efficiency. For example, IDaaS can automatically handle downstream application account creation and deletion for employees during their onboarding and offboarding.

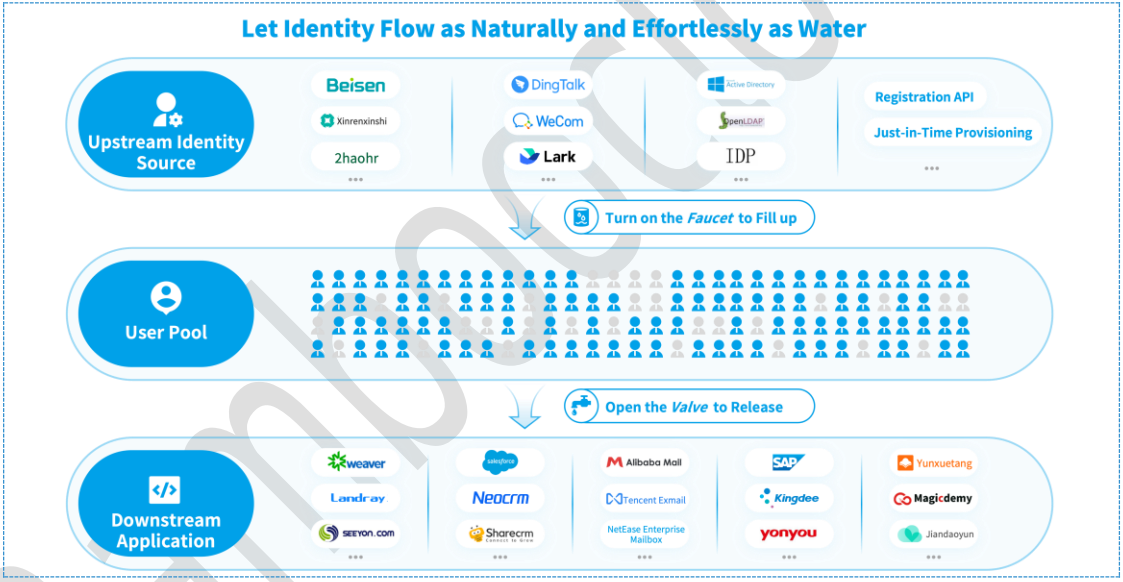
With traditional identity management models, enterprises may face the following challenges:

- **Inefficient account provisioning for onboarding**: When new employees join, application administrators must manually create accounts for each application, which leads to slow account provisioning that can impede business operations.
- **Delayed account deprovisioning for offboarding**: When employees depart, application administrators must manually delete accounts for each application. Any delays or oversight in this process may result in former employees retaining access to core enterprise systems, creating security vulnerabilities.

To address these pain points, IDaaS integrates with enterprise HR systems as the upstream identity source, synchronizing the organizational structure, personnel data, position information, and other related data to the IDaaS user pool in real time. Based on dimensions such as organization structures, user groups, and user attributes, enterprises can flexibly define authorization policies as needed.

Without manual intervention, IDaaS can automatically create, update, and delete accounts, ensuring real-time identity data synchronization between the upstream identity source and downstream business systems. This resolves issues related to poor timeliness, low efficiency, and human errors while addressing associated security vulnerabilities.

Additionally, IDaaS can identify and clean up non-compliant accounts (such as dormant accounts, duplicate accounts, and orphan accounts), thereby reducing risks of sensitive data theft and leaks. By enhancing the flexibility, precision, and security of system access and permission management, IDaaS facilitates smooth business operations and efficient workflows.



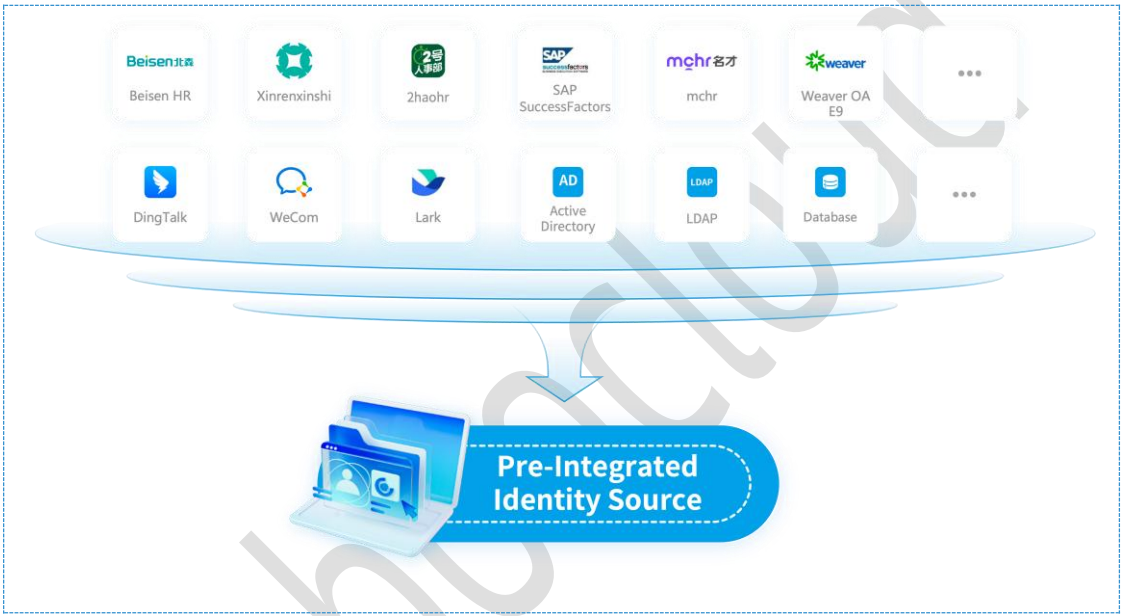
4. 1. 1 Upstream identity source

To meet the management needs of both internal employees and external business partners, IDaaS has pre-integrated with various mainstream identity sources. No code modifications are required—enterprises can import their organizational structures and personnel information from existing HR systems into the IDaaS user pool through simple configuration.

Once the enterprise's HR system is integrated with IDaaS, all HR events such as onboarding, position changes, internal transfers, and offboarding

can be synchronized to IDaaS in real time to ensure the accuracy and timeliness of identity data.

The pre-integrated upstream HR identity sources include Beisen HR, Xinrenxinshi, 2haohr, mchr, eRoad HR, WorkTrans HR, Weaver OA E9, DingTalk, WeCom, Lark, Microsoft Active Directory (AD), Lightweight Directory Access Protocol (LDAP), SAP SuccessFactors, and databases.



4. 1. 2 Unified registration

For scenarios involving the management of individual consumers and members, IDaaS offers a unified registration service that allows individual users to register through various channels such as the official website, membership system, and consumer applications using phone numbers, email addresses, or social media accounts.

By consolidating identity data from multiple sources, IDaaS helps enterprises establish global user OneIDs, build a standardized identity repository, and achieve cross-platform identity data governance.

To further streamline the registration process for individual users, IDaaS supports Just-in-Time (JIT) provisioning: when users log in to IDaaS for the

first time, IDaaS automatically creates a platform account for them and authenticates their identity. If users already have a platform account, they are directly authenticated.

Additionally, IDaaS has pre-integrated with mainstream social platforms as authentication sources, enabling users to quickly log in with their social media accounts. This provides a seamless registration and login experience and can significantly improve user registration rates.

Throughout the entire user registration, login, and use process, IDaaS delivers personalized cross-platform user experiences and helps enterprises build a high-performance, high-availability individual user management system driven by big data.

4. 1. 3 Downstream system identity synchronization

IDaaS supports a variety of international standard protocols and mechanisms for enterprises to effortlessly integrate business systems with IDaaS, achieving seamless identity synchronization between upstream and downstream systems.

When identity-related events occur in the upstream HR system (such as onboarding, position changes, internal transfers, or onboarding), IDaaS automatically synchronizes the latest identity data to all downstream business systems, eliminating delays and errors caused by manual IT operations.

Meanwhile, IDaaS is pre-integrated with over 1000 commercial applications, allowing enterprises to achieve smooth identity data integration through simple configuration.

For internal employee and external business partner management, the supported identity synchronization protocols and mechanisms include SCIM, LDAP, AD, event callbacks, and identity APIs. For individual customer and member management, the supported synchronization protocols and

mechanisms include registration APIs, JIT provisioning, and webhooks.

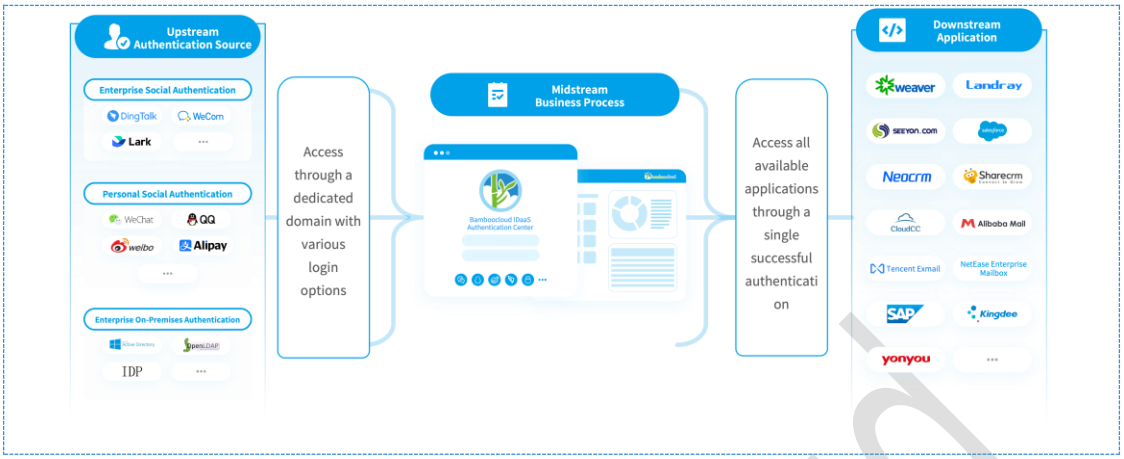
4. 2 Unified authentication

The unified authentication service allows users to efficiently and securely access all authorized business systems using a single set of credentials.

In traditional enterprise IT environments, users typically have separate credentials for different business systems. Overly complex passwords can lead to frequent password reset requests as employees may forget them, increasing the operational burden on IT administrators. Conversely, overly simple passwords or reusing the same password across multiple systems may result in security vulnerabilities, increasing the risk of data breaches and security incidents.

With the unified authentication service, users can access all authorized business systems after authenticating with a single set of credentials only once, enabling authentication resources to be shared across different systems. Furthermore, IDaaS pre-integrates multiple passwordless authentication methods, such as social login via QR code, verification code, and biometric recognition. Administrators can easily configure and flexibly combine different authentication options as needed.

Additionally, enterprises can configure password policies based on their security standards to mitigate the risks of weak or reused passwords and enhance identity security. Meanwhile, IDaaS offers a self-service portal allowing users to reset their passwords independently without relying on IT administrators, thus reducing the workload on IT departments.



4. 2. 1 Authentication methods

IDaaS offers various flexible authentication methods, including social login, enterprise on-premises authentication, passwordless authentication, and device authentication, to fully meet the identity authentication needs in diverse scenarios.

4. 2. 1. 1 Social login

IDaaS pre-integrates mainstream social authentication sources. Enterprise administrators can enable the corresponding social login method in the management console based on the needs of different business systems.

Through the IDaaS platform's diverse social login options, users can freely choose their preferred social accounts for QR code login without relying on traditional username-password authentication methods, significantly enhancing the user experience.

Pre-integrated personal social login options include Sina Weibo, Alipay, Douyin, Apple ID, Taobao, WeChat, and QQ. Pre-integrated enterprise social login options include DingTalk, WeCom, Lark, WeLink, Cloud Hub, and Weaver eteams.

4. 2. 1. 2 Enterprise on-premises authentication

IDaaS can integrate with enterprises' on-premises authentication systems

(such as AD domain authentication or authentication platforms based on standard protocols). Therefore, enterprises can continue using their existing authentication systems to maintain users' familiar workflows.

IDaaS pre-integrates multiple enterprise-grade authentication sources that comply with standard protocols, allowing flexible configuration based on business needs without any additional code modifications or development.

If an enterprise is using AD domain services, administrators can configure IDaaS to route authentication requests to the enterprise's AD domain. When users enter their AD domain credentials on the IDaaS login interface, the authentication request is automatically forwarded to the AD domain. Upon successful authentication, users gain access to their target business systems.

IDaaS also supports federated authentication with authentication products based on SAML or OIDC protocols, ensuring enterprises can retain their existing login interface.

The supported enterprise on-premises authentication sources include SAML, OAuth, LDAP, CAS, OIDC, Kerberos, and AD.

4. 2. 1. 3 Passwordless authentication

As password-cracking technologies evolve, even complex passwords meeting security standards cannot completely mitigate the risk of compromise. Traditional password-based authentication is gradually being replaced by more secure alternatives, with passwordless authentication emerging as the dominant trend in identity authentication.

The core concept of passwordless authentication is to minimize reliance on static and easily crackable passwords in favor of authentication factors that are more difficult to steal or replicate. This approach fundamentally addresses security vulnerabilities such as password breaches, leaks, or

misuse.

IDaaS platform incorporates various passwordless authentication methods, such as social login via QR code, verification code, dynamic one-time password (OTP), and biometric recognition based on the FIDO standard. These options help enterprises significantly enhance authentication security and meet the requirements of modern security frameworks.

The supported passwordless authentication methods include SMS verification code, email verification code, dynamic OTP, FIDO, QR code scanning, and social login via WeChat, QQ, Sina Weibo, Alipay, Douyin, Apple ID, Taobao, DingTalk, WeCom, Lark, WeLink, Cloud Hub, and Weaver eteams.

4. 2. 1. 4 Device authentication

IDaaS supports centralized authentication management for enterprise hardware devices such as VPNs and NAS to create an integrated authentication management framework that incorporates both devices and business systems.

IDaaS is compatible with hardware products from major vendors such as Huawei, Sangfor, H3C, TOPSEC, Fortinet, and Cisco, allowing rapid integration of network devices such as VPNs, virtual desktops, and bastion hosts using the RADIUS protocol.

To address common security risks associated with remote work, IDaaS supports step-up authentication methods (such as dynamic OTP and biometric recognition), further securing remote device access and ensuring enhanced identity security for enterprises.

4. 2. 2 Single sign-on

Single sign-on (SSO) is an authentication and authorization mechanism that enables users to securely access all authorized business systems with

a single login.

IDaaS supports multiple international standard protocols, such as SAML, OAuth, OIDC, and CAS, and provides SDKs in multiple programming languages to help enterprises' development teams quickly integrate applications and implement SSO.

Through the IDaaS platform's SSO service, internal employees, business partners, and individual customers can access all available systems without repeated logins. This streamlined access process significantly improves daily operational efficiency.

The supported SSO protocols and mechanisms include SAML, OAuth 2.0, OIDC, CAS, WS-Federation, and SSO APIs.

4. 2. 2. 1 Multiple entry points

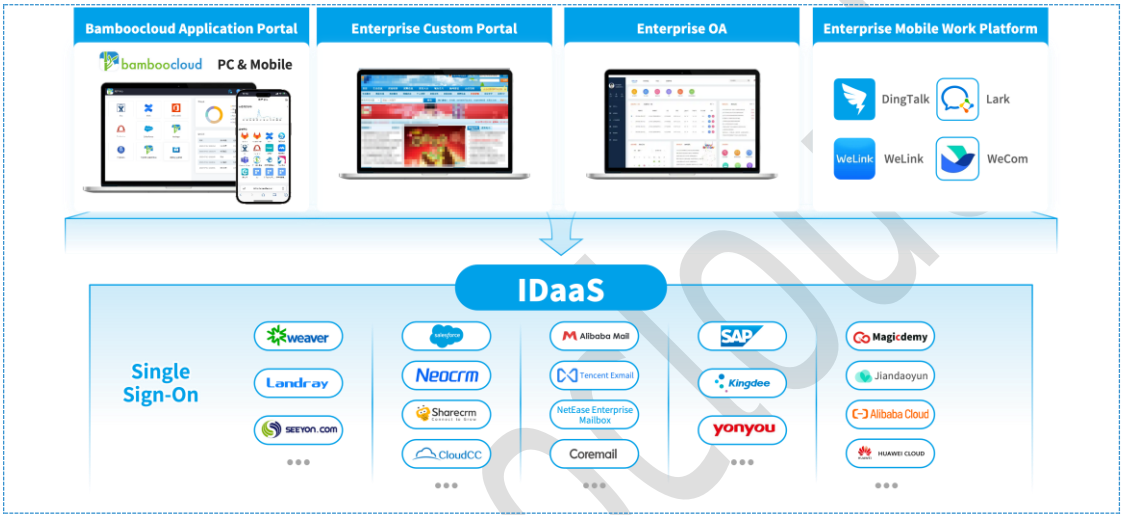
IDaaS offers various and flexible entry points to meet users' diverse needs. Users can access through either the target system's URL or the IDaaS default web or mobile HTML5 application portal. After authentication, users can view the list of all business systems to which they have been granted access.

In addition to the default application portal (user center), IDaaS also supports integrating SSO URLs of various business systems into enterprises' custom portals or office automation (OA) workspace. This allows secure and convenient SSO without changing existing workflows and user habits while simplifying the access process to business systems.

To address mobile work needs, IDaaS is fully compatible with the three mainstream enterprise mobile office platforms in China (DingTalk, WeCom, and Lark). By integrating business system SSO URLs to the mobile office platforms' workspaces, IDaaS serves as a bridge enabling seamless passwordless login from mobile office platforms to common business systems and SaaS applications. This provides enterprises with a more

convenient, efficient, and secure mobile work solution.

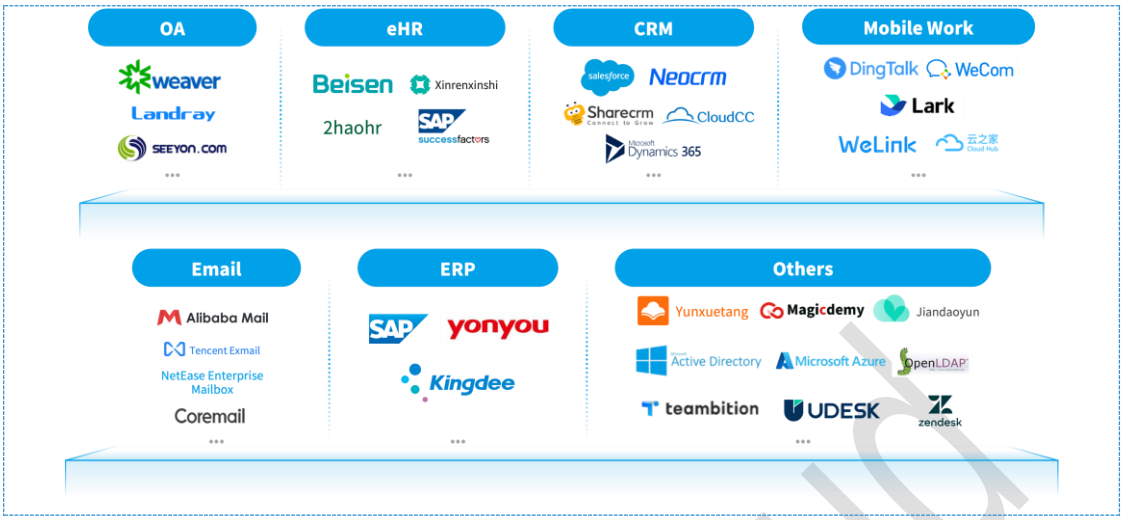
The supported entry points include the IDaaS default web and mobile HTML5 application portal, enterprises' custom portals, enterprise OA systems, and enterprise mobile office platforms (such as DingTalk, WeCom, Lark, and WeLink).



4. 2. 2. 2 Application ecosystem

IDaaS has pre-integrated with over 1000 commercial applications, extensively covering enterprise operations and business scenarios including collaboration platforms, customer relationship management (CRM) systems, human resource management (HRM) systems, mobile work systems, email systems, and enterprise resource planning (ERP) systems.

For pre-integrated applications, integration can be completed quickly without any code modification, significantly reducing the costs of development, operations, and maintenance. This streamlines integration processes, enhances efficiency, and maximizes the value of business and data.



4. 2. 3 Multi-factor authentication

Multi-factor authentication (MFA) is a more secure authentication mechanism that requires users to prove their identities using a second authentication method after completing password verification, thereby effectively safeguarding the security of both internal business systems and SaaS applications.

Even if user credentials are compromised, the enforced MFA can serve as a critical defense against unauthorized access, significantly reducing the risk of identity theft and preventing sensitive data breaches.

IDaaS supports policy-based MFA configuration, allowing administrators to flexibly define MFA trigger rules as needed. For example, administrators can determine the scope of users subject to MFA based on the organizational structure, user groups, specified user lists, or user attributes. These can be combined with multi-dimensional conditions such as time periods, device types, geographic locations, authentication methods, and risk behaviors, to implement fine-grained authentication management.

The supported dimensions and specific conditions for configuring multi-factor authentication policies are as follows.

Dimension	Condition
Time period	● Any time ● Within a specified period ● Outside a specified period
Device type	● Browser: Google Chrome, Microsoft Internet Explorer, Firefox, or others ● PC operating system: Windows, Linux, macOS, or others ● Mobile operating system: iOS, Android, or others
Geographic location	● Any location ● Within a specified location ● Outside a specified location
Authentication method	● Any authentication method ● Specified authentication method ● Non-specified authentication method
Risk behaviors defined by administrators	● Unusual location ● Unusual device ● Unusual IP address ● Locked account

IDaaS offers a variety of multi-factor authentication methods that enterprises can flexibly configure and combine based on the security requirements of their business systems. For example, stronger authentication methods such as OTP or FIDO-based fingerprint recognition can be used for core financial systems such as ERP.

The supported multi-factor authentication methods include SMS

verification code, email verification code, Google Authenticator OTP, Microsoft Authenticator OTP, Bamboocloud Castle OTP (WeChat mini program), and biometric authentication based on FIDO.

Adaptive multi-factor authentication

While rule-based MFA can effectively ensure access security for business systems, it may create usability friction for users who need to log in frequently. To address this, IDaaS offers a risk-based adaptive MFA mechanism that balances user experience and access security.

With adaptive MFA, IDaaS continuously evaluates users' login environment risks in real time and dynamically adjusts authentication policies based on the assessed risk level. If any suspicious activities or potential risks are detected, IDaaS automatically elevates the authentication level and requires users to complete step-up authentication. Conversely, if IDaaS determines that the user is in a trusted environment, only a single authentication step is needed for quick access.

For example, when a user logs in from the same geographic location or using the same device, IDaaS considers this a trusted environment and allows login without additional authentication.

However, IDaaS enforces MFA in the following scenarios:

- Login from an unusual geographic location
- Login from a new device
- Login using a new IP address

By dynamically adjusting authentication policies, IDaaS helps enterprises effectively mitigate potential risks while enhancing the overall user experience. For more details about risk assessment, refer to the Risk management section.

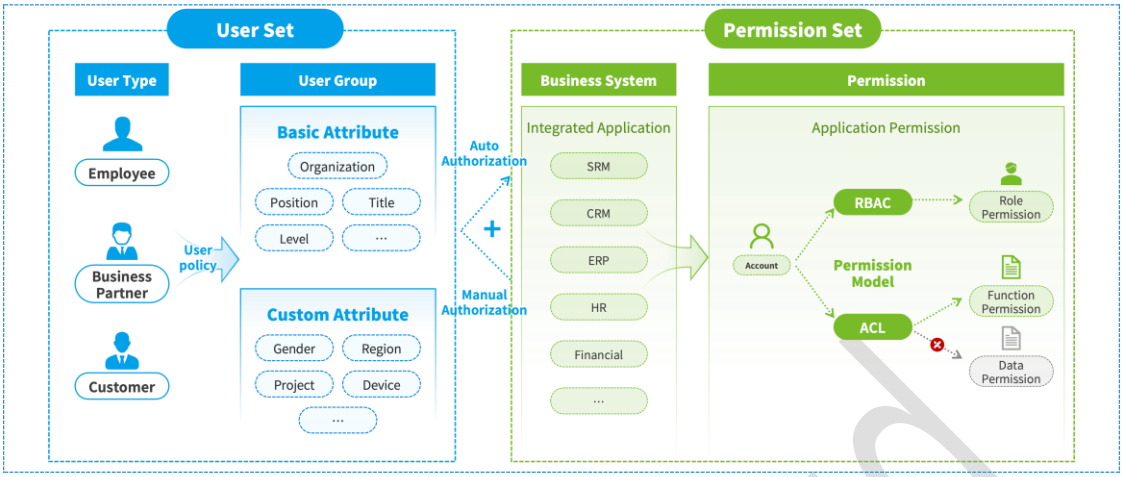
4. 3 Permission management

As enterprises continue to expand their digital systems and workforce, the information environment is becoming increasingly complex and posing significant challenges for permission management.

For users, requesting permission typically involves multiple platforms and lengthy approval processes, which often results in inefficiencies. For administrators, permission management tasks are scattered across different business systems, each with its own distinct permission model. Also, manual management is prone to improper permission assignments, delays in permission revocation, or permission misuse.

Regular security audits of user permissions are critical for ensuring compliance and identifying potential risks. However, the inconsistent permission management approaches among internal business systems make it difficult to perform unified compliance reviews of permission management processes and permission data. This leads to a lack of effective compliance measures both within and across systems.

To address these challenges, IDaaS provides granular permission management for business systems with industry-standard role-based access control (RBAC) and access control list (ACL) models. By combining automatic policy-based authorization with manual authorization, IDaaS delivers a centralized management view of accounts, roles, and permissions for downstream business systems.



With a centralized permission management portal, IDaaS simplifies the permission-related process for users, administrators, and compliance auditors. This enhances operational efficiency, prevents security vulnerabilities caused by human errors, and ensures regulatory compliance throughout the permission assignment process.

Administrators can also implement flexible authorization tailored to different scenarios. For enterprise-wide systems or those governed by clear standard rules, permissions can be automatically assigned based on dimensions such as organizational structures, user groups, roles, job positions, and user attributes. For critical business systems, a hybrid approach combining offline approvals and online manual authorization can be adopted to meet the strict security and precision requirements in complex scenarios, reducing risks such as excessive authorization or unauthorized access.

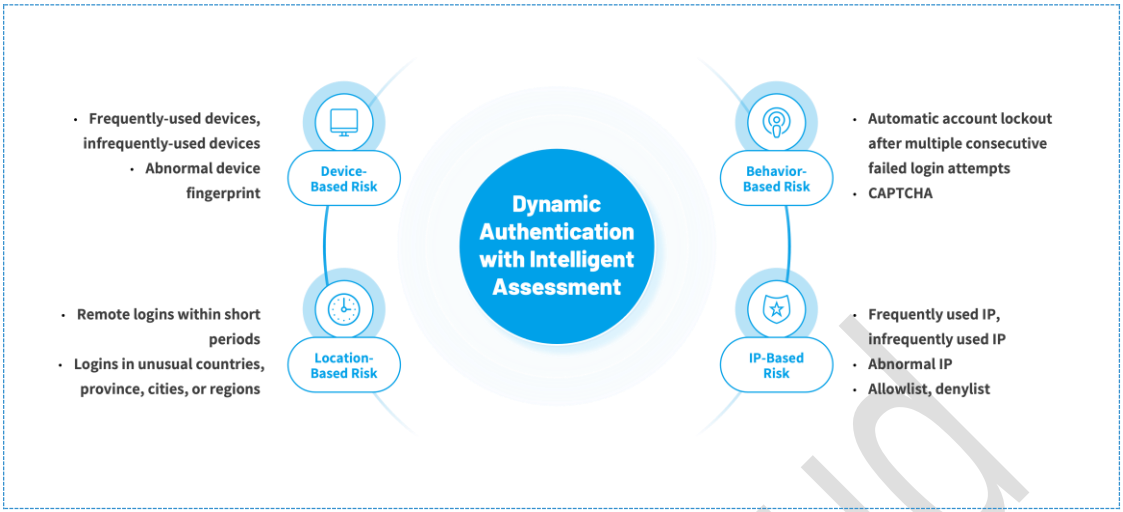
IDaaS optimizes permission management workflows and provides flexible authorization models to address enterprise needs across diverse business contexts. By resolving common challenges such as difficulty in provisioning, querying, revocation, and management of permissions, IDaaS ensures efficient, intelligent, and compliant authorization while enabling seamless business operations.

4. 4 Risk management

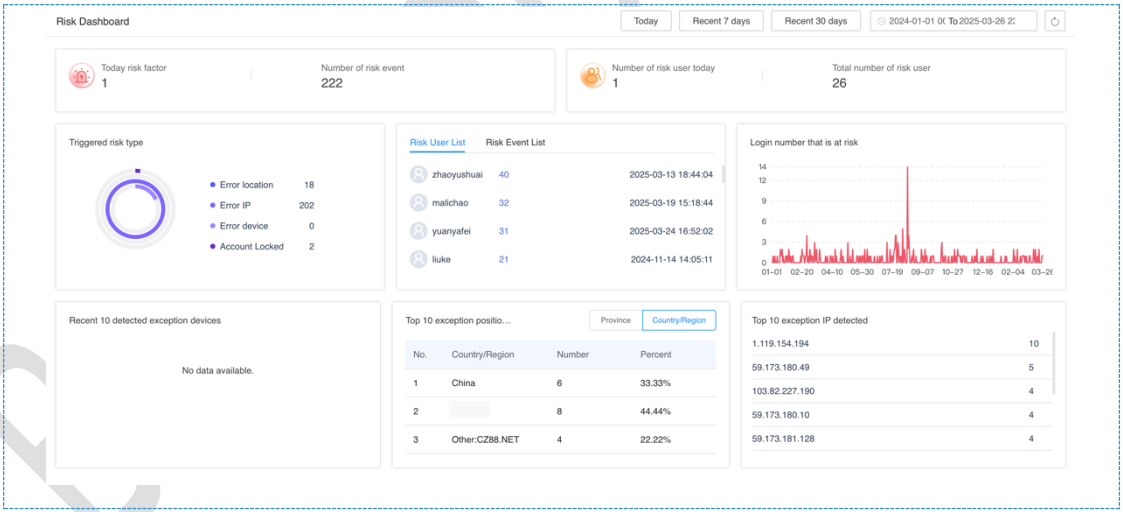
As workplace environments become increasingly diverse, enterprise identity governance scenarios grow more complex and face a higher prevalence of identity theft and fraud attacks. Traditional passive defense methods struggle to address the security challenges in today's digital era. Using intelligent detection mechanisms for automatic identification, proactive alerts, and timely risk mitigation has become a key focus in strengthening identity security defenses and a new direction for risk management solutions.

IDaaS features a built-in risk control engine that continuously performs dynamic identity security risk assessment based on multiple dimensions including user identities, device characteristics, network environments, and business operations. The system enforces corresponding security policies and control measures according to different risk scenarios, blocks suspicious login attempts in real time, and effectively prevents malicious cyberattacks, ensuring secure access to business systems by only legitimate users.

When risk behaviors are configured as conditions for authentication policies, risk-based adaptive MFA can be implemented. This approach optimizes the user login experience while enhancing security, striking a balance between protection and convenience.



IDaaS provides visual risk data reports that display real-time statistics of security incidents. This helps management teams and security personnel understand overall security risk posture more intuitively, comprehensively, and efficiently, while providing data-driven insights for decision-making in security operations.



4. 5 Compliance audit

To better address enterprise needs in compliance auditing and business data management, IDaaS offers comprehensive identity audit services including login logs, operation logs, and visualized reports across all scenarios.

4. 5. 1 Compliance audit logs

IDaaS provides end-to-end logging and log export capabilities for user operations, administrator operations, and SMS and email notifications, which fully satisfies enterprise compliance audit requirements and facilitates security incident investigation and root cause analysis.

User operation logs

User operation logs record user login authentication and self-service operations.

- **Login authentication logs**: Record the login time, location, authentication method, and the accessed business system.
- **Self-service operation logs**: Record the login time, location, and self-service operations (such as password changes, personal information updates, phone number or email address changes), along with operation results (success or failure). If the operation fails, the failure reason is also recorded.

Administrator operation logs

Administrator operation logs record all administrator operations in the management console, including the operation time, location, and operation details.

SMS and email notification logs

SMS and email notification logs record all notifications sent to users via the IDaaS built-in or external SMS and email gateways. Logs include the sending time, recipient user, notification content, and specific scenarios where notifications are sent.

Log export

If the enterprise is using a professional security information and event management (SIEM) platform, it can synchronize the IDaaS logs to the

SIEM platform through the following methods.

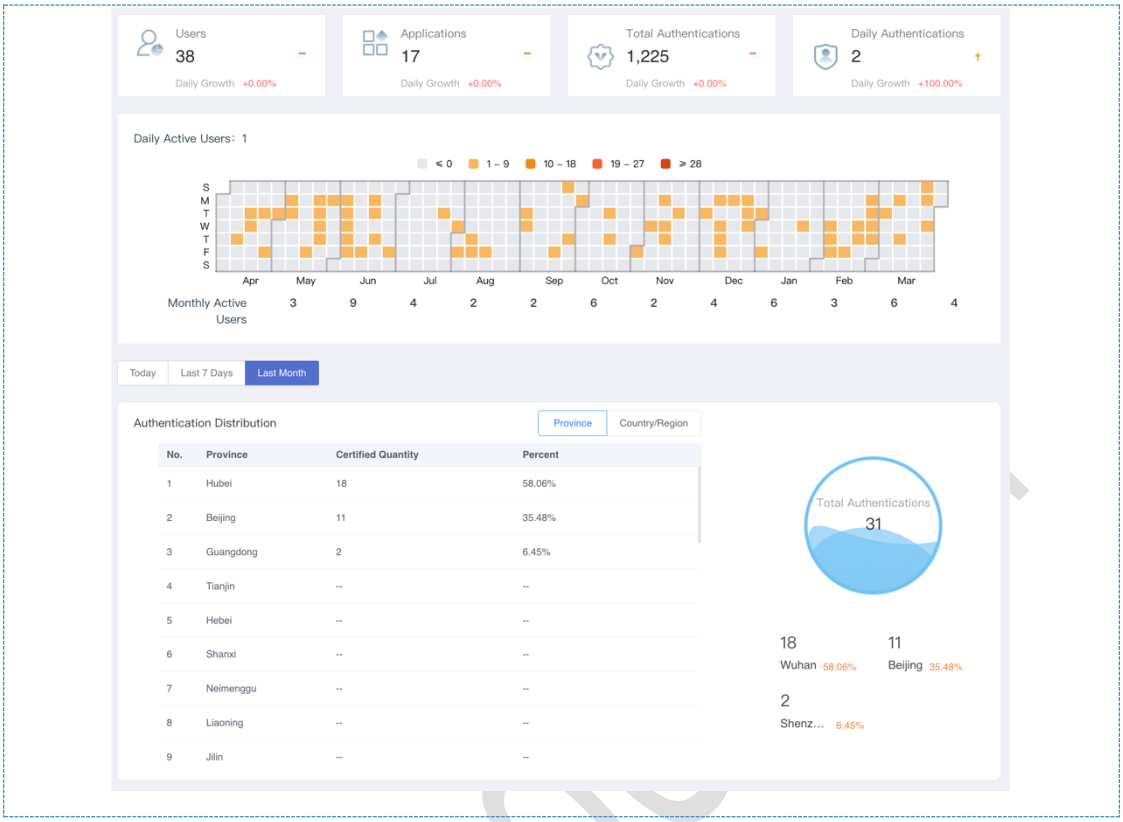
- **Manual batch export**: All audit logs can be batch exported offline for archiving and further analysis.
- **Automatic API synchronization**: Enterprises can use the audit log APIs of IDaaS to automate log synchronization and reduce manual operations.

4. 5. 2 Visual charts

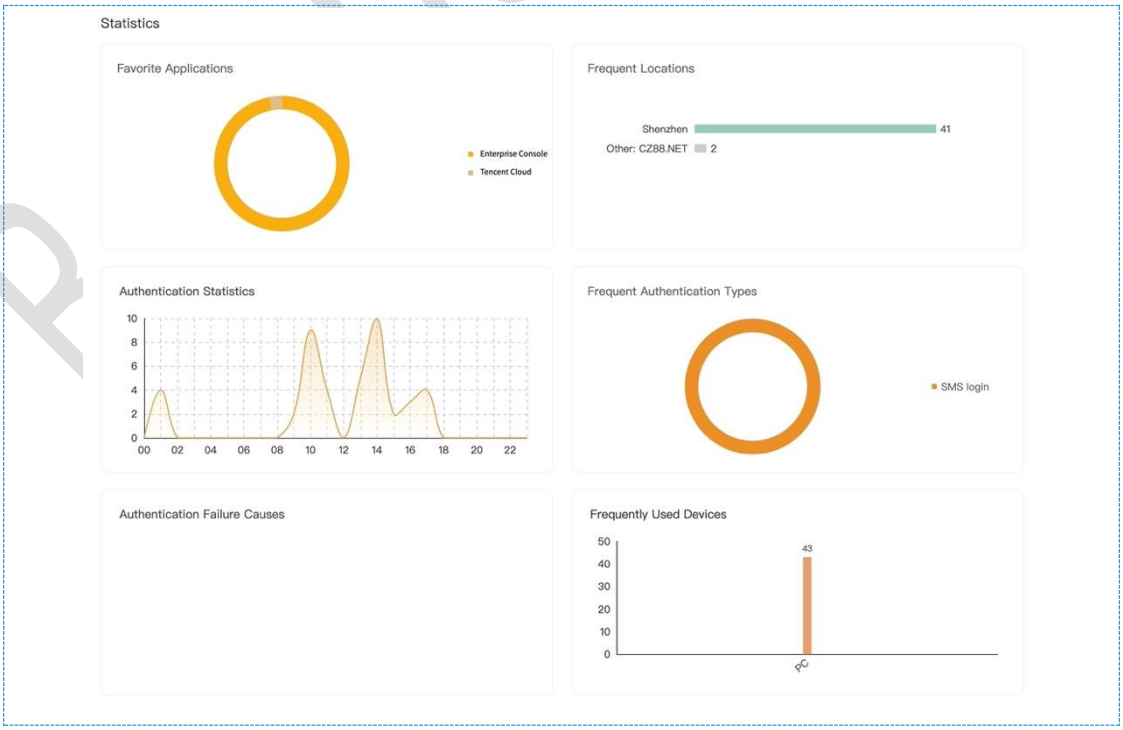
IDaaS provides multi-dimensional visual charts that help administrators quickly grasp the overall authentication status of the enterprise. For example, administrators can visually monitor daily and monthly user activity data or analyze authentication behavior patterns based on users and applications to further optimize authentication management strategies.

The provided visual charts illustrate the following data:

- Total enterprise user and unactivated user counts
- Total application count
- Cumulative authentication count
- Daily authentication count
- Daily active user and monthly active user counts
- Authentication distribution map by country and region
- Authentication trend based on time
- Top 10 users by authentication frequency
- Top 10 users by authentication failure
- Authentication method distribution
- Top 10 applications by access volume
- Device and browser usage distribution



Additionally, IDaaS provides various visual charts for users to view their preferred authentication methods and related statistics.



5 Networking solutions for application integration

Before integrating business systems with the IDaaS, enterprises need to develop an appropriate network connection plan based on the deployment location of the business systems and the enterprise's network security policies, balancing access efficiency with security requirements.

5. 1 For applications deployed in internal networks

For business application systems deployed in internal networks, IDaaS offers three network connection options: direct connection mode, cloud bridge mode, and proxy mode.

Direct connection mode

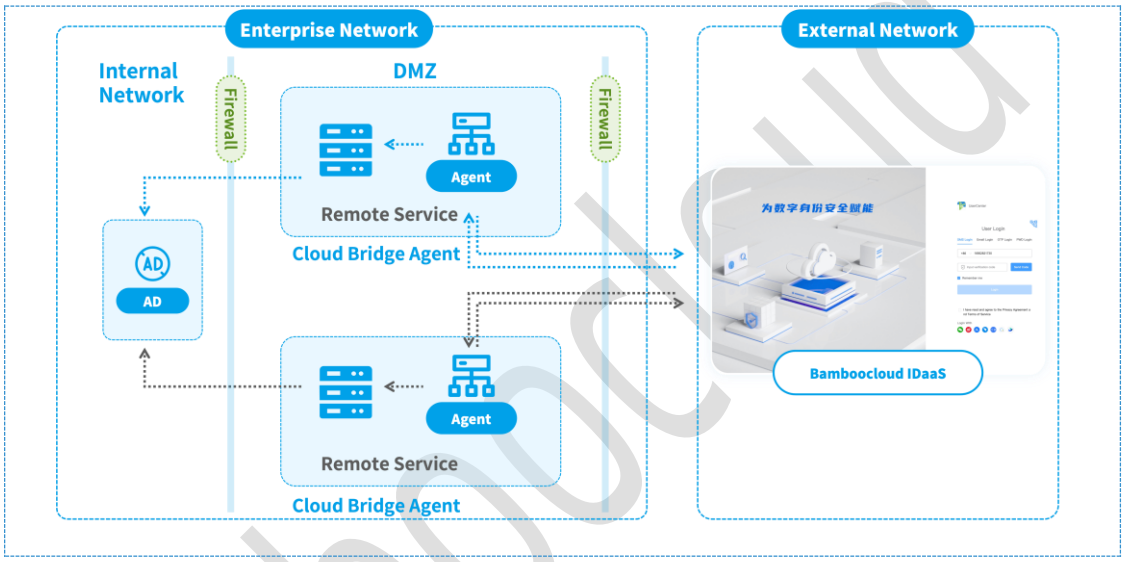
If the enterprise allows both inbound and outbound network policies for internal business systems, these systems can directly communicate with IDaaS through bi-directional network requests. The enterprise's network administrator needs to configure the network policy and allowlist the source IP addresses of IDaaS requests, ensuring that only requests from IDaaS can access the internal business systems.

Cloud bridge mode

For enterprises that do not allow internal services to be directly exposed to the public network (in other words, inbound access to the intranet is prohibited), a cloud bridge can be deployed to enable bidirectional data communication between internal business systems and IDaaS. The cloud bridge creates a reverse connection to IDaaS, forwards IDaaS requests to

internal business systems (such as AD), and returns the system's responses to IDaaS.

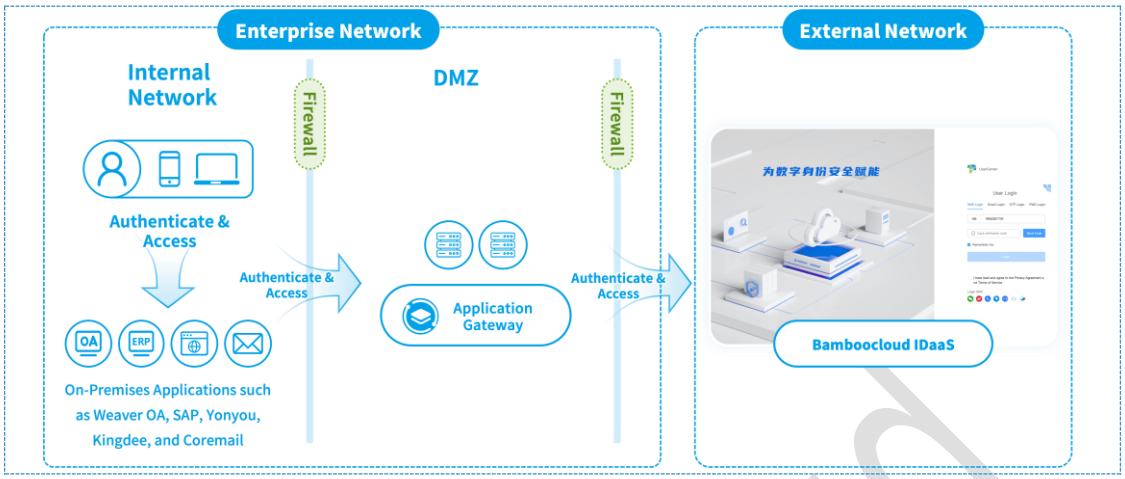
For higher security, it is recommended to deploy the cloud bridge within the internal network if outbound access is allowed. If outbound access is prohibited either, the cloud bridge needs to be deployed in the demilitarized zone (DMZ).



Proxy mode

In scenarios where outbound access is prohibited and users can access business systems only through the internal network, enterprises can integrate business systems with IDaaS via proxy mode: installing an agent gateway in the DMZ and using local DNS services to map the IDaaS domain to this gateway, with network communication enabled between the proxy gateway and IDaaS.

Through proxy mode, users can indirectly access IDaaS, achieving identity synchronization and unified authentication while meeting the enterprise's network isolation security requirements.



5. 2 For applications deployed in external networks

Business systems hosted on mainstream cloud platforms (such as Alibaba Cloud, Huawei Cloud, or Tencent Cloud) and third-party SaaS applications can inherently access the public internet. This means that these systems can directly establish network connections with IDaaS, enabling rapid integration without additional network configuration.

6 Appendices

6. 1 Pre-integrated applications

The following are some office systems and SaaS applications pre-integrated in IDaaS.

6. 1. 1 Office management

weaver	Weaver e-cology 9.0		Weaver eteams
	Landray EKP		Landray MK
SEEYON.com	Seeyon OA	Active Directory	Active Directory
	DingTalk Professional		DingTalk Enterprise
	WeCom		Lark Enterprise
Alibaba Mail	Alibaba Mail		Tencent Exmail

网易 企业邮箱	NetEase Enterprise Mailbox		Coremail
	RichMail	263	263 Enterprise Mail
	Yunsu Mailbox	WeLink	WeLink
云之家 Cloud Hub	Cloud Hub		WPS Office
	Microsoft 365		Office 365
	Teambition	Worktile	Worktile
	Wenjuan.com		FangCloud

6. 1. 2 Human resources

	Beisen HR		Xinrenxinshi

	2haohr		Moka
	SAP SuccessFactors		mchr
	eRoad HR		WorkTrans HR

6. 1. 3 Financial management

	SAP-GUI		SAP NetWeaver
	SAP S/4 HANA Cloud		SAP Concur
	SAP Ariba		Yonyou NC
	Yonyou NC Cloud		Yonyou NCV65
	Yonyou U8		Kingdee Jingdouyun

Kingdee	Kingdee Constellation	Kingdee	Kingdee Galaxy
	HOSE	Maycur	Maycur
	DiDi Enterprise Solutions		Z-trip
	Helios	ORACLE	Oracle E-Business Suite

6. 1. 4 Communication and collaboration

	VooV Meeting Enterprise		Zendesk
zoom	Zoom Enterprise		

6. 1. 5 Marketing management

salesforce	Salesforce	Sharecrm Connect to Grow	Sharecrm
Neocrm	Neocrm	CloudCC	CloudCC

	Dynamics 365		Yichuang CRM
	Sobot		SAP Cloud for Customer
	Oracle Sales Cloud		Veeva CRM

6. 1. 6 Development and design

	Amazon Web Services		Microsoft Azure
	Alibaba Cloud		Tencent Cloud
	Huawei Cloud		Kingsoft Cloud
	Baidu AI Cloud		JD Cloud
	Jiandaoyun		GitLab

	Jenkins		ZenTao
	Jira		Redmine
	Zabbix		JumpServer
	Qizhi		Alibaba Cloud RAM
	Grafana		

6. 1. 7 Data and analytics

	FanRuan BI		Tableau
	GuanData BI		ESENSOFT BI

6. 1. 8 Education and training

	Magicdemy		Times Bright CreSuccess

	Yunxuetang		Confluence

6. 1. 9 Security and compliance

	Eagle Cloud		DACS
	Zscaler		QIYUESUO
	SecureLink		

6. 2 Abbreviations

ACL	Access Control List
AD	Active Directory
API	Application Programming Interface
CI/CD	Continuous Integration and Continues Delivery
CAS	Central Authentication Service
CIAM	Customer Identity and Access Management
CRM	Customer Relationship Management
DDoS	Distributed Denial of Service
DMZ	Demilitarized Zone

EIAM	Enterprise Identity and Access Management
ERP	Enterprise Resource Planning
FIDO	Fast Identity Online
HR	Human Resources
HRM	Human Resource Management
HTML	Hypertext Markup Language
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ID	Identity
IDaaS	Identity as a Service
IP	Internet Protocol
IT	Information Technology
IoT	Internet of Things
JIT	Just-in-Time
LDAP	Lightweight Directory Access Protocol
MFA	Multi-Factor Authentication
OA	Office Automation
OAuth	Open Authentication
OIDC	OpenID Connect
OTP	One-Time Password
RADIUS	Remote Authentication Dial-In User Service
RBAC	Role-Based Access Control

SAML	Security Assertion Markup Language
SCIM	System for Cross-domain Identity Management
SDK	Software Development Kit
SSO	Single Sign-On
TLS	Transport Layer Security
VPN	Virtual Private Network
WAF	Web Application Firewall