tanflow

TANFLOW IAM SUITE

VERSION: 10.0.1

TANFLOW VENTURES
PRIVATE LIMITED

What is Tanflow IAM Suite?

Tanflow IAM Suite is a robust and scalable Identity and Access Management (IAM) platform, offering three core application stacks: Identity Management, Access Management, and Directory Services. It is designed to streamline user lifecycle management, secure access to resources, and ensure compliance with modern security standards.

Core Application Stacks

1. **Identity Management**
   The Identity Management module focuses on managing user identities and their lifecycle. Key features include:
   - User Management: Comprehensive control over user accounts, attributes, and profiles.
   - Provisioning and Deprovisioning: Automated management of user access across systems.
   - Password Management: Strong password policies and password dictionaries to enhance security.
   - Notification Management: Configurable alerts for user activities.
   - Dynamic Policies: Context-aware access policies tailored to organizational needs.
2. **Access Management**
   The Access Management module ensures secure and seamless access to resources. Its capabilities include:
   - Single Sign-On (SSO): Unified authentication across multiple applications.
   - OAuth 2.0 & SAML 2.0: Support for modern authentication standards.
   - Multi-Factor Authentication (MFA): Enhanced security for user logins.
   - Role-Based Access Control (RBAC): Fine-grained control over permissions.
   - Attribute Mapping: Flexible integration with external systems.
3. **Directory Services**
   The Directory Services module provides a centralized repository for storing and managing identity-related data. Features include:
   - LDAP Integration: Seamless connectivity with LDAP-based systems.
   - High-Performance Storage: Efficient and scalable management of identity data.
   - Audit Logging: Comprehensive logging for compliance and troubleshooting.

Additional Functionalities

Tanflow IAM Suite comes with a wide range of additional features:

- Dynamic Group Management: Manage groups dynamically based on user attributes.
- Self-Enrollment: Simplified user onboarding process.
- Recertification Campaigns: Periodic reviews of user access to ensure compliance.
- Provision Applications: Streamlined application provisioning and deprovisioning workflows.
- Useful Links Management: Centralized management of external resource links.

Business Benefits of Tanflow IAM Suite?

- Protects sensitive data with robust authentication mechanisms like MFA, SSO, OAuth 2.0, and SAML 2.0.
- Enforces strong password and dynamic access policies, reducing vulnerabilities.
- Automates provisioning and deprovisioning processes, saving time and reducing errors.
- Centralizes user management, enabling efficient control over user identities and roles.
- Ensures adherence to regulatory requirements with detailed audit logs and recertification campaigns.
- Provides customizable policies for password, access, and user activities to meet compliance standards.
- Implements Single Sign-On (SSO) for seamless access to multiple applications, improving user experience.
- Offers flexible integration with external systems through directory services and attribute mapping.
- Accommodates growing business needs with a scalable and modular design.
- Adapts to diverse organizational requirements with customizable policies and configurations.
- Automates repetitive tasks like group management, notifications, and provisioning, freeing up IT resources.
- Reduces the total cost of ownership (TCO) by consolidating identity, access, and directory services into a unified platform.
- Provides quick and secure access to resources, enabling employees to focus on their work.
- Offers self-enrollment and self-service capabilities to reduce dependency on IT support.
- Supports dynamic group management and role-based access control (RBAC) to maintain organizational hierarchy.
- Provides periodic recertification campaigns to ensure only authorized users retain access.

Technology Benefits of Tanflow IAM Suite?

- Seamlessly integrates with modern protocols like OAuth 2.0, SAML 2.0, and LDAP.
- Designed to handle growing user bases and application demands with scalable architecture.
- Unifies user, policy, and directory management into a single platform.
- Automates user provisioning, group management, and policy enforcement.
- Supports advanced security features like Multi-Factor Authentication (MFA).
- Provides flexible and dynamic access control policies for enhanced security.
- Enables Single Sign-On (SSO) for seamless authentication across applications.
- Offers customizable workflows and policy configurations to suit business needs.
- Ensures high availability and reliability with robust system architecture.
- Supports detailed logging and audit trails for compliance and troubleshooting.
- Adapts to emerging technologies with modular and future-ready design.
- Enhances application provisioning with attribute mapping and directory integration.
- Provides high-performance data handling for identity and directory services.
- Streamlines integration with external systems through APIs and attribute mapping.
- Offers self-service options for users to reduce IT dependency.

Features of Tanflow IAM Suite?

Identity Management Module

User Management

- Centralized management of user accounts and attributes.
- Role-based access control (RBAC) to define user permissions.
- Self-Enrolment options for user onboarding.
- Bulk user import/export functionalities for efficient data handling.
- Flexible user attribute configurations with custom fields.
- Account lifecycle management including activation, suspension, and deletion.
- Add User – Create new user profiles with default & custom attributes.
- Edit User – Update/modify existing user profiles.
- Delete User – Remove accounts with safeguards.
- View User – View detailed profiles incl. assigned apps & groups.
- Activate/Deactivate User – Temporarily disable/restore access.
- Import Bulk Users – CSV-based bulk onboarding.
- Modify Bulk Users – Apply updates to multiple users (except username/org).
- Delete Bulk Users – Bulk deletes via usernames.
- Export – Export selected user data (CSV).
- Export All Users – Export complete user database.
- Set/Reset Password – Assign/reset user passwords.
- Import Groups – Bulk assign users to groups via CSV (multi-app support, validation, error logs).
- Export All Groups – Export all groups with users & applications.
- Lock Account – Temporarily lock/unlock accounts for security.

Provisioning and Deprovisioning

- Automatic provisioning of user accounts across integrated systems.
- Deprovisioning workflows to revoke access upon user exit.
- Role-based provisioning to assign resources dynamically.
- Integration with HR systems for seamless onboarding and offboarding.
- Automatic provisioning of user accounts across integrated systems.
- Deprovisioning workflows to revoke access upon user exit.
- Role-based provisioning to assign resources dynamically.
- Integration with HR systems for seamless onboarding and offboarding.
- Add Provision Application – Configure provisioning via DB, API, or LDAP; set credentials; map attributes; enable Create/Update/Delete sync.
- Edit Application Provision – Modify provisioning method, mappings, sync actions, and server details.
- View Application Provision – View app details, config, mappings, and assigned provision group/users.

- Reconciliation – Compare IDAM vs target system data; detect missing or mismatched users/attributes.
- Perform Synchronization – Sync to create, update, disable, or delete users as per config.
- Activation/Deactivation Provision Application – Pause/resume provisioning without deleting config.

Password Management

- Strong password policy enforcement with customizable rules.
- Password dictionary to prevent weak or commonly used passwords.
- Self-service password reset functionality for users.
- Account lockout policies to prevent brute-force attacks.
- Strong password policy enforcement with customizable rules.
- Password dictionary to prevent weak or commonly used passwords.
- Self-service password reset functionality for users.
- Account lockout policies to prevent brute-force attacks.
- Create Password Policies – Define rules (length, complexity, expiry, history).
- Apply Password Policies – Assign policies to organizations/LDAP configs.
- Edit Password Policies – Update existing policy rules.
- Delete Password Policies – Remove policies (only if unassigned).
- Review Applied Policies – View which orgs have specific policies applied.
- Enable/Disable Password Dictionary – Toggle common-password blocking.
- Upload Password Dictionary File – Upload .txt list of disallowed passwords.
- Password Validation Check – System checks entered password against dictionary + rules.

Dynamic Group Management

- Automatic group assignments based on user attributes.
- Support for nested groups to simplify hierarchical management.
- Dynamic updates to groups as user attributes change.
- Add Policy & Condition – Define conditions, group type (SSO/App Groups), and associated group; users onboarded are provisioned based on these dynamic policies.
- Re-evaluate Policy – Sync non complaint users (users are not in the group and0020matching policy = non-compliant;)

Notification Management

- Configurable alerts for account changes, login attempts, and policy violations.
- Email notifications for critical events.
- Customizable templates for user and admin notifications.
- Create Notifications – Define title & message; launch now or schedule for later.
- Target Audience – Choose specific organizations (comma format) or all users.
- Notification Display in Portal – Visible in user portal based on org/role, appears under Notifications section as clickable links.
- Control Link Visibility – Active/Inactive toggle to temporarily hide/show notifications without altering config.

Access Management Module

Single Sign-On (SSO)

- Unified access to multiple applications with a single login.
- Support for popular SSO protocols like SAML 2.0 and OpenID Connect.
- Centralized management of SSO-enabled applications.
- Secure token-based authentication with OAuth 2.0.

Multi-Factor Authentication (MFA)

- MFA enforcement for critical applications and sensitive data.
- Support for multiple MFA methods including TOTP, Email, SMS, FIDO.

Authorization and Attribute Mapping

- Attribute-based access control (ABAC) for fine-grained resource permissions.
- Flexible attribute mapping for integrating external directories.
- Role-to-attribute mapping for seamless access control configuration.

Advanced Features

Recertification Campaigns

- Run campaigns to regularly review user access.
- Multi-level workflow: User self-review → Manager → Auditor.
- Automated email reminders at each step.

Provisioning Applications

- Automated provisioning for third-party applications.
- Support for attribute mapping and transformation during provisioning.
- Custom workflows for application-specific provisioning needs.

Attribute and Policy Management

- Centralized attribute repository for user data across modules.
- Configurable policy templates for access and password management.
- Real-time policy updates for immediate enforcement.

Configuration

- Organize user profiles into clear sections (General Info, Office Info, etc.).
- Add custom fields (attributes) tailored to your organization's needs.
- Create dropdowns or hierarchical lookups (e.g., Country → State → City).
- Auto-fill attributes based on conditions (e.g., if Org = X, User Type = Y).

Notification and Alert Systems

- Send announcements and alerts directly to users inside the IDAM portal.
- Schedule notifications or publish them instantly.
- Target specific organizations or share with everyone.
- Users see real-time updates under their “Notifications” tab.

Useful Links

- Admins can share important links (documents, training, portals) with selected users or all users.
- Links can be launched immediately or scheduled for later.
- Users see only the links relevant to their role or organization.

Email Management

- Configure email delivery settings (SMTP) to ensure smooth communication.
- Use customizable email templates for events like password resets, welcome emails, or recertification, etc.
- Track email delivery status and resend failed messages if needed.

Access Requests (Requester)

- Users can request access to applications, groups, or roles with justifications.
- HR or Managers can request new user accounts or updates to user details.
- Request MFA resets securely if a user lost/broke device.
- Track request status (Pending, Approved, Rejected, Completed) for transparency.

Approvals

- Requests follow a multi-level approval chain (Manager → Final Approver).
- Approvers can review, modify, approve, or reject requests easily.

Orphaned Accounts

- Detect inactive or orphaned accounts (e.g., unused logins).
- Define rules based on attributes like last login date.
- Edit or delete rules as policies change.

Technical Specifications

1. Centralized Identity and Access Management (IAM) Solution with Single Sign-On (SSO)

A unified system that enables users to securely authenticate and access multiple applications and systems with a single set of credentials, eliminating the need for multiple logins and enhancing user convenience.

2. Access Permissions Linked to Role Definitions

Permissions and privileges are assigned based on predefined role definitions rather than individual user accounts. Access control is determined by role membership, ensuring consistent and scalable access management.

3. Support for Federation Protocols

Compatibility with widely used federation standards, including Security Assertion Markup Language (SAML), Active Directory Federation Services (ADFS), OAuth, and OpenID Connect, to facilitate secure integration and identity sharing across platforms.

4. Scalability for Large User Bases

Designed to handle up to 200,000 users, with seamless integration across multiple applications and solutions, ensuring performance and reliability even under heavy load.

5. Real-Time Authorization Decisions

Provides immediate and course-grained access control decisions for user requests, ensuring secure and efficient application access.

6. Role-Based Access Control (RBAC) for Application Functionalities

Implements RBAC to manage and restrict access to specific features and functions within applications based on user roles.

7. Automated User Onboarding and Lifecycle Management

Integrates with HR systems like SAP ERP to automatically onboard new employees, update role assignments, and deactivate accounts upon termination.

8. Self-Service Password Reset with Enforced Policies

Allows users to reset their passwords independently while adhering to predefined password strength and security policies.

9. Recovery of Forgotten Credentials

Facilitates the recovery of forgotten login credentials through automated email notifications, reducing dependency on IT support.

10. Auto-Discovery and Synchronization of User Data

Ensures consistent user data across multiple identity sources by automatically discovering and synchronizing updates.

11. Generation of Unique, Permanent User Identifiers

Assigns a unique and immutable identifier to each user for consistent tracking and management across systems.

12. Comprehensive Audit and Logging Capabilities

Tracks and logs all user activities for enhanced accountability, security monitoring, and compliance reporting.

13. Automated Archival of Audit Logs

Archives audit logs automatically after a predefined period, ensuring efficient data management and compliance with retention policies.

14. Predefined Reporting Capabilities

Offers out-of-the-box reports on user access, role assignments, and orphaned accounts for quick insights into access management.

15. High Availability and Disaster Recovery

Ensures uninterrupted service through load balancing, failover configurations, and disaster recovery mechanisms.

16. Integration with Directory Services

Supports seamless integration with directory services like Active Directory (AD), Lightweight Directory Access Protocol (LDAP), and other similar systems.

17. Multi-Factor Authentication (MFA)

Enhances security by implementing MFA using methods such as one-time passwords (OTPs), mobile app tokens, and biometric authentication.

18. Advanced Authentication Mechanisms

Supports modern authentication options like Time-Based One-Time Passwords (TOTP) and email-based authentication for enhanced flexibility.

19. Dynamic Access Rights Adjustments

Automatically adjusts access rights based on role changes, predefined schedules, or business rules to maintain compliance.

20. Enforced Password Policies

Implements strict password policies, including strength requirements, expiration schedules, and reuse limitations, to enhance security.

21. Session Timeout and Automatic Logout

Provides configurable session timeout settings and automatically logs out inactive users to reduce security risks.

22. Browser-Independent Solution

Ensures seamless operation across different web browsers and platforms for a consistent user experience.

23. Configurable Welcome Screens

Displays personalized welcome screens with login history, user alerts, and other relevant information.

24. Unsuccessful Login Attempt Notifications

Notifies users of failed login attempts and enforces account lockout policies after multiple failed attempts.

25. Notifications for Access Rights Changes

Alerts users about changes to their access rights or potential policy violations to maintain transparency and awareness.

26. Automated Provisioning and De-Provisioning

Streamlines user provisioning and de-provisioning processes based on lifecycle events such as role changes or employment status updates.

27. Integration with Diverse Applications

Provides seamless compatibility with third-party, custom-built, and enterprise-grade applications for broader adoption.

28. Connector Availability for Target Systems

Offers connectors for major systems to simplify and accelerate integration with the IAM solution.

29. Real-Time User Access Monitoring

Includes dashboards and Management Information System (MIS) reports for continuous monitoring and detailed insights into user access.

30.Role Synchronization Across Applications

Ensures consistent role assignments and synchronization between integrated applications and the IAM system.

31.Secure Account Activation and Deactivation Mechanisms

Implements secure processes for activating or deactivating user accounts upon request to minimize risks.

32.Support for IPsec Connections and Network Optimization

Enables secure IPsec connections, optimizes network bandwidth, and ensures reliable cloud connectivity.

33.Approval Workflows for Access Requests

Supports configurable approval workflows and routing rules to streamline and secure access request processes.

34.Scheduled User Account Audits

Conducts periodic audits of user accounts and access rights to maintain a robust security posture.

35.Notifications for Inactive Accounts

Automatically identifies and notifies administrators about inactive accounts with detailed records for remediation.

36.Future-Ready Solution

Designed to scale and accommodate additional users and integrations without significant disruptions or reconfiguration efforts.

37. Bulk User Import & Modification

Upload CSV files to create or update hundreds of users at once, saving time for onboarding and role changes.

38.Bulk User Deletion

Remove inactive or separated users in bulk with safeguards to avoid accidental data loss.

39.Account Locking & Unlocking

Temporarily lock accounts during suspicious activity or compliance checks, with secure unlock workflows.

40.View & Export User Profiles

Administrators can export selected or all user details for audits, reporting, and system migrations.

41.Hierarchical Organization Structures

Support parent-child organizations with inherited password/security policies.

42.Custom Role Definitions

Flexible creation of roles with description and granular permissions.

43.Role Deletion Safeguards

Roles can only be deleted once all users are unassigned, preventing accidental access disruptions.

44.Self-Service Access Requests

Employees can request new applications, roles, or group memberships without IT intervention.

45.Multi-Level Approval Workflows

Requests pass through two or more approvers (Manager → Admin → Auditor) before access is granted.

46.Automated Policy-Driven Provisioning

Users are automatically assigned to groups or applications based on attributes (e.g., department, location).

47.Configurable Notifications & Links

Admins can broadcast system updates, training material, or alerts with scheduling and audience targeting.

48.Custom Email Templates

Predefined triggers (welcome, reset password, recertification) with branding support.

49.Email Delivery Monitoring

Real-time logs of successful/failed emails with retry options.

50.Custom Attributes & Sections

Organizations can define their own user data fields and organize them into sections (e.g., General Info, HR Info).

51.Lookups & Multi-Level Lookups

Self-Define dropdowns and hierarchical lookups (Country → State → City) for structured data entry.

52.Smart Populate Rules

Automatically fill attributes (e.g., user type, department) based on conditions during onboarding.

53.Provisioning via Database, API, or LDAP

Flexible sync methods for integrating with third-party systems.

54.Reconciliation Reports

Detect mismatched or missing users between IDAM and external systems.

55.On-Demand Synchronization

Manual “Sync” button to align user data instantly.

56.Segregation of Duties (SoD) Rules

Prevent conflicting access combinations (e.g., “cannot be both approver and requester”).

57.Recertification Campaigns

Periodic reviews of user access by managers, auditors, and users themselves.

58.Orphan Account Detection

Automated identification of inactive or unmanaged accounts based on rules (e.g., last login date).

59.Password Dictionary Enforcement

Blocks common or weak passwords using uploaded blacklists.

60.Comprehensive Audit Logs

Track every login, change, and admin action for compliance.

61.Predefined & Downloadable Reports

Out-of-the-box reports for login success/failures, orphan accounts, and policy compliance.

62.Bulk Operations Tracking

Jobs dashboard with progress bars, error logs, and categorization (In-progress, Completed, Failed).

Contact Information

TANFLOW VENTURES PRIVATE LIMITED

tanflow

Address

DCG01-310, DLF CORPORATE GREENS, SECTOR 74A, GURGAON, HARYANA, 122002

Email
contact@tanflow.com

PARTNERS:

BITCHIEF TECHNOLOGY SERVICES PRIVATE LIMITED

IBTS

TECH-CENTRICS IT PRIVATE LIMITED

TECH-CENTRICS