

Feature	Description
CIAM – Customer Identity & Access Management	
Customer Registration & Onboarding	Supports registration and onboarding of retail customers.
Customer Profile Management	Enables customers to manage identity attributes and profile information.
Self-Service Account Management	Allows customers to manage profiles, credentials, sessions, and account settings.
Email and SMS OTP-Based Registration & Authentication	Allows users to log in using an OTP sent to their email/SMS. New users are created in ZTrust after successful verification.
Social / External Identity Login	Supports authentication through external identity providers and social media accounts such as Google, LinkedIn, Facebook, Instagram, Twitter etc.
Customer MFA	Provides multi-factor authentication for customer applications.
Customer Passwordless Authentication	Enables secure passwordless authentication for customer identities.
Consent & Preference Integration	Supports integration with consent and preference management capabilities.
WIAM – Workforce Identity & Access Management	
Workforce Identity Management	Manages employee and workforce identities throughout their lifecycle.
Joiner-Mover-Leaver (JML)	Automates identity changes when employees join, move roles, or leave the organization.
Workforce SSO	Provides centralized single sign-on for workforce applications.
Workforce MFA	Enforces multi-factor authentication for workforce users.
HRMS Integration	Integrates workforce identity lifecycle processes with HR systems such as zoho people.
AD / LDAP Support	Integrates with Directory services, fetches users and authorizes them via ZTrust.
IGA – Identity Governance & Administration	
Access Request Management	Allows users to request access to applications and resources.
Approval Workflows	Routes access requests through configurable approval workflows.
Role Requests	Allows users to request application or Line-of-Business roles.
Access Reviews	Supports periodic review of user access.
Access Certification	Enables managers or administrators to certify assigned access.
Segregation of Duties (SoD)	Helps identify and manage conflicting access combinations.
Role Governance	Supports controlled assignment and management of roles.
B2B IAM – Business-to-Business Identity Management	
Partner Identity Management	Manages identities belonging to business partners.
Vendor & Supplier Identity Management	Supports external vendor and supplier identities.
External Organization Onboarding	Onboards users and organizations outside the enterprise.
Delegated Administration	Allows external organizations or delegated administrators to manage their users.
Partner SSO & Federation	Provides federated access for partner organizations.
Non-Human Identity Management	
Service Accounts	Manages identities used by services and automated processes.
Application Identity Management	Manages application and client identities.
API Identity Management	Supports identity and authentication for APIs.
Workload Identity	Supports identity for workloads and machine-based processes.
Machine-to-Machine Authentication	Enables secure authentication between applications and services.
MFA & Passwordless	
Multi-Factor Authentication (MFA)	Supports OTP, TOTP, MPIN, biometric, NFC/RFID, QR code and push notification multi factor authentications for enhanced login security.
Contextual & Risk-Based Authentication	Dynamically adapts authentication based on location, device, and behavior.
Passwordless Authentication	Enables authentication without requiring traditional passwords.
Offline TOTP Authentication	Enables authentication without internet connectivity using time-based one-time passwords.
Authenticator App	Provides TOTP, push approvals, QR login, NFC and biometric authentication through the authenticator application.
Customizable Authentication Workflows	Allows authentication flows to be defined based on application, user, or group requirements.
reCAPTCHA Protection	Helps prevent automated attacks and bot logins during authentication.
Brute Force Attack Detection	Detects repeated failed login attempts and applies configurable lockout policies.
Password Management Policies	Supports password complexity, expiration, and credential reuse policies.
ZTrust Authenticator	Available for Android and iOS, supporting MFA and passwordless authentication.
SSO & Federation	
Single Sign-On (SSO)	Provides centralized authentication across multiple enterprise applications.
SAML 2.0	Supports SAML-based identity federation and single sign-on.
OpenID Connect (OIDC)	Supports modern identity federation and authentication using OIDC protocol.
OAuth 2.0	Supports delegated authorization and token-based access.
Federated Identity Support	Unifies authentication across applications and external identity providers.
External Identity Provider Integration	Integrates ZTrust with external identity providers.

Authorization & Access Management	
Granular Access Policies (RBAC/ABAC)	Provides fine-grained access control based on roles, attributes, or group membership.
Role-Based Access Control (RBAC)	Controls access to resources based on assigned roles.
Attribute-Based Access Control (ABAC)	Controls access using user, resource, environment, and contextual attributes.
Fine-Grained Permissions	Defines granular permissions for resources and actions.
Group-Based Access Control	Controls access using group membership.
Application Roles	Defines and manages roles specific to applications.
Composite Roles	Combines multiple roles into higher-level roles.
Identity Lifecycle Management	
Directory Sync & User Lifecycle Management	Synchronizes users from AD/LDAP and automates provisioning and deprovisioning.
User Onboarding	Creates and onboards identities into the identity platform.
Provisioning & Deprovisioning	Automates granting and revoking access throughout the identity lifecycle.
Identity Reconciliation	Reconciles identity information across connected systems.
User Import & Export	Supports bulk import and export of user identities using structured files, enabling administrators to efficiently onboard and transfer user information.
Directory Services Integration	
Active Directory Integration	Integrates ZTrust with Microsoft Active Directory.
LDAP Integration	Connects ZTrust with LDAP directories.
SCIM 2.0	Supports standardized identity provisioning and synchronization.
Enterprise Application Integration	Connects ZTrust with enterprise applications.
REST APIs	Provides APIs for identity, application, role, and access integration.
Integration Guide	Provides step-by-step guidance with code snippet for integrating applications with ZTrust.
Multi-Tenant IAM	
Tenant / Realm Management	Manages multiple isolated identity domains.
Realm Isolation	Separates identities, applications, roles, and configurations between tenants.
Realm Administrators	Supports delegated administration for individual tenants.
Realm Specific Users, Roles & Applications	Manages identity resources specific to each tenant.
Centralized Administration	Provides centralized administration across all Realms.
Self-Service Identity Management	
Self-Service Portal	Allows users to manage profiles, passwords, sessions, and access requests.
User Profile Management	Allows users to view and update supported profile information.
Device Management	Allows users to view, register, and remove authenticator devices associated with their account.
Session Management & Invalidation	Allows administrators or users to manage and terminate active sessions.
Role Requests (App & LoB Level)	Allows users to request roles at application or Line-of-Business level.
Profile Photo Management & Sync	Allows users to upload profile photos or synchronize supported external profile photos.
Identity Audit & Compliance	
Audit Trails & Custom Event Logs	Tracks user and administrative actions with timestamps and descriptive event information.
Comprehensive Reporting	Generates and exports reports such as active users, locked users, and login trends.
Compliance & Logging	Supports audit logging and integration with enterprise logging mechanisms.
Authentication Audit	Records authentication events for monitoring and investigation.
Authorization & Access Audit	Tracks authorization and access-related activities.
Administrative Audit	Tracks administrator actions across the identity platform.
Real Time Admin Dashboard	Provides graphical visibility into system activity, login trends, and security metrics.
Additional Security Capabilities	
Geo-Fencing & Geo-Tagging	Enforces location based access policies by defining allowed geographical login zones.
Time Fencing	Enforces schedule based access by allowing authentication only during predefined time windows.
Persistent Sessions	Maintains user sessions across restarts or upgrades for uninterrupted access.
Consent Management	
Default Consents	Provides predefined consent templates for applications.
Consent Versioning	Changes to consents are saved as new versions.
Parent-Child Consent Versions	Maintains relationships between consent versions.
Consent Archive & Unarchive	Allows consents to be archived and restored.
Audit-Preserving Storage	Archived consents are retained for audit and cannot be deleted.
Consent Response History	Stores all accepted and denied consent responses.
Version-Specific Responses	Links each response to the consent version presented to the user.
Application Consent Templates	Allows applications to invoke consent templates during user interactions.
Consent Capture	Captures and stores user consent responses from applications.
SSP Consent Management	Allows users to view their consents through the SSP.
Consent Withdrawal	Allows users to withdraw their consent through the SSP.
Supported Deployment Platforms	
Supported Deployment Platforms	Kubernetes, OpenShift, Azure AKS, AWS ECS, AWS EKS, Google GKE, and virtual machine (VM) environments.

On-Premises / Data Center	Supports deployment within enterprise data center environments.
Disaster Recovery (DR)	Supports deployment architectures for disaster recovery and business continuity.
High Availability (HA)	High Availability through internal caching via infinispn, clustering and External Load Balancers
Password Management & Policies	
Password Policies	Configurable password complexity, length, expiration, and reuse policies.
Password Management	Allows users to securely change and manage their passwords.
Forgot Password / Password Reset	Allows users to securely reset forgotten passwords.
Password Expiration	Enforces password expiration based on configured policies.
Password History	Prevents users from reusing previously used passwords.
Password Lockout	Locks accounts after configured failed authentication attempts.
Password Change Verification	Requires additional verification such as OTP or security questions when changing a password.
Security & Cryptography	
Password Hashing	Enables secure password hashing using Argon2, PBKDF2, pbkdf2-sha512 and pbkdf2-sha256 algorithms.
Hashing	SHA-256, SHA-384, SHA-512, and SHAKE256.
Encryption	AES-GCM and AES-CBC encryption algorithms.
Digital Signatures	RSA, ECDSA, PSS, EdDSA, and HMAC-based signatures.
Certificate Manager	Manages TLS/SSL certificates for secure external identity integrations and TLS/SSL connectivity
Compliance & Standards	
Compliant on	GDPR, DPDP, FAPI 1.0 Advanced, FAPI 2.0, FIPS 140-2, ISO QMS (9001), ISMS (27001), ITSM (20000)
Add on Features	
Customizable Themes	Allows customization of login page themes and branding.
Customizable Email Templates	Allows customization of email templates for user communications.
Notifications	Supports notifications for relevant user and administrative events, such as role requests and approval actions.
Broadcast News	Allows publishing announcements and broadcast messages to users.
Monitoring & Analytics	
System Overview	Provides real-time metrics for CPU, memory, threads, uptime, and garbage collection.
Identity Metrics	Provides metrics for users, groups, clients, and active sessions.
System Monitoring	Provides visibility into system health and runtime performance.
Version & Update Check	Checks for the latest ZTrust version and available updates.
Realm Overview	Provides a consolidated overview of realm-level users, groups, clients, sessions, and authentication activity etc.