Accops HyID – Identity-first access control with contextual MFA, SSO, and audit-ready governance

B

Advanced Identity and Access Management Solution

HyID is a comprehensive Identity and Access Management (IAM) solution that safeguards corporate resources, critical business applications, and data from internal and external threats.

It secures access through multi-factor authentication (MFA), single sign-on (SSO), contextual access controls, and centralized identity governance to ensure that only authorized users can access enterprise systems.

Functioning as a cloud-native Identity Provider (IdP), HyID supports Authentication, Authorization, and Audit (AAA) requirements across modern and legacy environments, enabling consistent identity policy enforcement across desktops, servers, applications, remote access gateways, and cloud services. HyID supports flexible deployment models, including on-premises, managed cloud deployments, and hybrid deployments, allowing organizations to align identity controls with regulatory, security, and infrastructure requirements.

What HyID Protects

- Microsoft Windows Desktop Login
- Microsoft Windows Server Login
- RDP into Windows Desktops & Servers
- Linux Server Console and Remote Shell Access
- Web-based applications & legacy applications
- Remote Access Gateways
- SSL VPN, Firewalls, Managed Switches
- Any corporate application via REST API
- SAML-based applications, like Office 365 & Salesforce
- GSuite through 2FA or MFA
- Cloud-based applications and services

Multi-Factor Authentication (MFA)

HyID secures corporate resources with various authentication techniques, including:

- One-Time Passwords (OTP) via SMS, email, PC software, mobile app, TOTP and hardware tokens
- Biometric authentication: fingerprint and face recognition
- Push notifications for mobile and PC
- Security keys (FIDO2 and FIDO-U2F)
- **Magic Number feature** for additional security against automated attacks
- QR code-based authentication

HyID evaluates access risk using contextual factors such as user location, device posture, browser, access time, and behavior to determine the appropriate authentication level. Low-risk access can be granted through silent authentication, while higher-risk scenarios trigger step-up authentication. Administrators can tailor security policies to maintain the right balance between protection and user convenience.

Zero Trust Architecture Support

HyID forms a critical component in implementing Zero Trust security models by:

- Verifying user identity with multiple factors before granting access
- Acting as a centralized identity enforcement layer across applications, endpoints, and access channels
- Continuously authenticating users throughout their sessions
- Applying context-aware security policies based on user behavior and risk factors
- Supporting just-in-time and just-enough access principles

Desktop Login Protection

HyID provides robust protection for desktop and server logins:

- **Windows:** Secure login with MFA, including **face authentication** via Windows Credential Provider
- **Linux:** Secure console and shell access with MFA
- **RDP and SSH:** Require MFA for remote access to Windows and Linux systems

New features include:

- Face authentication for Windows desktop login
- Cred UI MFA support for administrative tasks
- Offline login support using mobile apps or hardware tokens
- Step-up authentication for privileged operations

Flexible Token Support

HyID supports a wide range of tokens and authentication methods:

- SMS OTP
- Email OTP
- Hardware tokens (OATH compliant)
- PC software tokens
- Mobile app tokens (iOS and Android)
- Biometric tokens (fingerprint, face)
- Security keys
- Push notifications (mobile and PC)

This flexibility enables organizations to select the most suitable authentication methods for their users and security requirements.

Availability and Deployment Options

HyID is available as a standalone product or as an add-on to HySecure. It supports high availability and failover, ensuring continuous operation. Deployment options include:

- On-premises installation
- Virtual private clouds (VPCs) in public clouds such as Azure and AWS
- Accops-managed cloud-based deployments
- Hybrid deployments with synchronized authentication policies

Privilege Access Audit & Control

HyID enables organizations to track, control, and audit privileged access. It ensures that users with administrative privileges are properly authenticated, and their actions are logged. Features include:

- Requiring personal domain accounts for privileged access
- Dynamic risk-based policies for additional authentication
- Detailed logging of privileged user activities
- Time-limited access for administrative functions

Integration Capabilities

HyID provides extensive integration options:

- REST-based API for easy integration with any application, enabling developers to add MFA to custom applications quickly
- SAML-based application support for seamless integration with popular services, such as Office 365 and Salesforce
- RADIUS integration for network equipment
- LDAP and Active Directory integration
- OAuth 2.0 and OpenID Connect (OIDC) support for modern application authentication
- Federation with external Identity Providers such as Azure AD and Okta

Network Security Integration

HyID integrates with network equipment using RADIUS and other protocols, such as SAML, to secure administrative access to firewalls, NAC devices, routers, and switches through strong authentication. Additional network security features include:

- IP-based access restrictions
- Geo-location filtering
- Network-based risk assessment
- VPN integration for secure remote access

Comprehensive Auditing & Monitoring

HyID offers comprehensive auditing and monitoring capabilities, tracking who accessed what resources, when, and from where. It provides:

- Detailed logs of authentication events
- Real-time monitoring dashboard
- Customizable alerts and notifications
- Endpoint details and risk assessments
- Integration with SIEM systems
- Compliance reporting

These capabilities enable organizations to maintain compliance and respond effectively to security incidents.

Key Differentiators

- **Seamless Desktop Login Protection:** Integrated face authentication for Windows desktops, enhancing security without compromising user experience.
- **Magic Number Feature:** An innovative MFA layer that thwarts automated attacks by requiring a unique, time-sensitive number.
- **Advanced IT Helpdesk Controls:** Flexible management options for administrators, including temporary access unlocks and user-specific configurations.
- **Offline Access Support:** Secure login capabilities even without internet connectivity, using mobile apps or hardware tokens.
- **Easy Application Integration:** REST API for straightforward integration of MFA into any application, ensuring broad compatibility.
- **Adaptive Authentication:** Context-aware policies that adjust security requirements based on risk factors.
- **User Self-Service Portal:** Enables users to register devices, reset passwords, and manage their authentication methods.

Compliance Support

HyID helps organizations meet compliance requirements for various regulations, including:

- DPDP
- GDPR
- HIPAA
- PCI DSS
- SOX
- NIST standards
- ISO 27001

Why Choose HyID?

HyID stands out in the identity and access management (IAM) market with its combination of identity platform capabilities, adaptive authentication, and broad integration support.

By securing access across desktops, servers, applications, and cloud services through a unified identity framework, HyID enables organizations to strengthen security while maintaining a seamless user experience.

Its cloud-native architecture, flexible deployment options, and context-aware access controls make HyID well-suited for enterprises operating in complex, hybrid IT environments.

Accops enables secure and instant remote access to business applications from any device and network, ensuring compliant enterprise mobility for business users while keeping governance with the organization.

Want to learn how Accops can help you secure critical applications, business data, and ensure compliance?
Reach us at contact@accops.com.