IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

ActivID® Authentication Appliance

STRONG AND VERSATILE AUTHENTICATION APPLIANCE

- **Increase security** – Decreases risks with robust two-factor authentication.
- **Enhance user convenience** – Multi-layer authentication that addresses user demands for convenience and portability.
- **Increase productivity** – Securely connects users from any location through a variety of devices and authentication methods.
- **Lower cost** – Versatile, future-proof authentication platform reduces the cost of fulfillment and management.
- **Extend value** – Enables secure access from smartphone, tablet, laptop and PC to VPNs, web portals and cloud applications.

HID Global’s ActivID® Authentication Appliance protects corporate, financial and government organizations with risk appropriate and cost effective user authentication that goes beyond passwords.

This solution gives end users a convenient experience for accessing sensitive resources from anywhere in the world, while using virtually any device, including their own smartphones, tablets or computers.

Deployment is simple, as the platform is already integrated with major cloud apps, VPN systems, application servers and other third party systems.

Organizations can also tailor their authentication methods to the needs of specific groups of users, providing each with the right balance of security, cost and convenience necessary to meet their business objectives, as well as ensure regulatory compliance and policy adherence.

It also supports the broadest range of authentication methods, from strong passwords to certificate-based authentication, including two-factor OATH standards-based hardware tokens, soft tokens, device forensics, SMS Out-of-Band One-Time Password (OTP) options and push-based authentication with mobile notifications.

The ActivID Authentication Appliance also supports HID Approve – our next-generation two-factor authentication solution that combines the security of public key-based cryptography with the convenience of mobile push notifications.

HID Approve delivers a simple and secure way for users to authenticate and verify their transactions. Available either on hardware or as a virtual appliance.

The ActivID® Authentication Appliance allows integration with HID Risk Management Solution, that uses machine learning and artificial intelligence to protect online transactions from a wide range of threats, including Fraudulent transactions, Account Take Over, Financial Malware and Man-in-the-browser (MitB attacks).

HID Risk Management also supports risk-based advanced authentication, allowing organization to deploy a highly secure authentication workflow that is transparent to the end user.
FEATURES:
- Natively integrated with HID Risk Management Solution for threat and fraud detection, and risk-based advanced authentication.
- Interoperable with HID Approve for push-based authentication with mobile notifications
- Organization-wide authentication solution with fine-grained authentication policies.
- Easily integrates with applications to leverage strong authentication.
- Digitally signed and sequenced audit logging and policies.
- Secure, highly scalable (from 100s to millions), resilient architecture.
- Enhanced security Domains provide strong segregation between different user populations.
- Works concurrently with legacy authentication servers for graceful and efficient migration.
- Integrates with Active Directory and most standard LDAP to match the scalability and availability of the organization's network (can be deployed with internal database when there is no existing LDAP).
- Flexible solution that allows organizations to generate their own security seed files for hardware token deployments.
- On-premise deployment to give organizations complete control over their data and environment.
- Tokens auto-synchronize to improve reliability and security and reduce support calls.
- Integrates seamlessly with full suite of credential management, middleware, smart card, single sign-on, mobility and physical access control offerings.
- Secure an organization’s keys by optionally connecting to a FIPS 140-2 network HSM.

SPECIFICATIONS

| Built-in Authentication Methods | HID Approve™ for public-key based authentication and transaction signing with push notification
| | One-time password (ActivIdentity patented algorithm) & Challenge / response
| | One-time password: OATH HOTP Event, TOTP Time-based, & OCRA challenge / response
| | OATH transaction signing (OCRA)
| | Smart Card PKI / X.509 certificate
| | Emergency full and partial strong Static Password & Security Questions
| | Out-Of-Band One-Time Password or Transaction Verification code sent via SMS or Email
| | Device ID - Web Browser Registration
| | Adaptive authentication with HID Risk Management Solution
| | Optional Threat and Fraud Detection with HID Risk Management Solution

| External Authentication Methods | LDAP fallback & passsthrough, RADIUS conditional routing

| Authenticators | Hardware Tokens
| BlueTrust Token, OTP Token, KeyChain OTP Token, Desktop OTP Token, Pocket OTP Token, Mini OTP Token, Any OATH compliant event, time or challenge / response-based hardware token, Smart Card (with ActivID CMS) – Including Crescendo C1100

| Software Tokens | Mobile and PC software token with HID Approve on iOS, Android, Windows 10

| User Repositories | Database
| Embedded Oracle® 12c with integrated fault tolerance
| Support for Microsoft Active Directory, Oracle / Sun Java Directory, Novell eDirectory

| Standards Supported | Protocols
| SAML v2, OpenID Connect, OAuth2, SCIM, RADIUS Authentication and Authorization, Web Services (SOAP), RESTful API over HTTP, LDAP v3, SNMP v3, syslog

| Cryptographic | OATH event, time and challenge / response, 3DES / AES / RSA / ECC / SHA-2
| FIPS 140-2 level 2 or level 3 network HSM (optional)/ Open Banking Security Profile

| Compliance Enablement | DFS 23 NYCCR 500, GDPR, FFIEC, OpenBanking, PCI DSS, PSD2

| Help Desk and Self Service | Web-based help desk & self service, Localizable & U.S. Section 508 compliant
| Administration | Device and Credential management, Authentication Policy management, User and Permission management

| Auditing, Accounting and Reporting | Digitally signed & sequenced tamper-evident audit log, Audit log queries, Published audit schema

© 2018 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, and ActivID are trademarks or registered trademarks of HID Global or its licensor(s)/supplier(s) in the US and other countries and may not be used without permission.

All other trademarks, service marks, and product or service names are trademarks or registered trademarks of their respective owners.


An ASSA ABLOY Group brand