IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

ActivID® Authentication Appliance

ActivID Authentication Appliance helps organizations improve productivity:

- Secure access from laptops, browsers, tablets, and smartphones using strong authentication
- Broad range of hardware and software authentication methods provide options and price points to best meet business needs
- Convenient and secure push notification based authentication with HID Approve
- Out-of-band authentication via SMS One-Time Passcodes or email ensures secure connectivity when other methods are not available
- Seamless integration with HID Risk Management Solution enables adaptive step-up authentication and account take-over protection

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 smart phones, 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 multi-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.

The ActivID® Authentication Appliance allow 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 trails.
- Secure, highly scalable (from 100s to millions), resilient architecture.
- 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 allowing organizations to leverage their existing user repository (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 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 (HID Global-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 Adaptive authentication with HID Risk Management Solution Optional Threat and Fraud Detection with HID Risk Management Solution
External Authentication	LDAP fallback & passthrough, 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, FIDO U2F and FIDO 2.0 devices, 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 **LDAP** Support for Microsoft Active Directory, Oracle / Sun Java Directory, Novell eDirectory
Standards Supported	**Protocols** SAML v2, OpenID Connect, OAuth2, SCIM, RADIUS Authentication and Authorization, FIDO, 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)/
	Compliance Enablement DFS 23 NYCRR 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

hidglobal.com

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +44 1440 714 850
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

© 2019 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.

2019-07-11-identity-assurance-activid-appliance-ds-en PLT-01178

An ASSA ABLOY Group brand