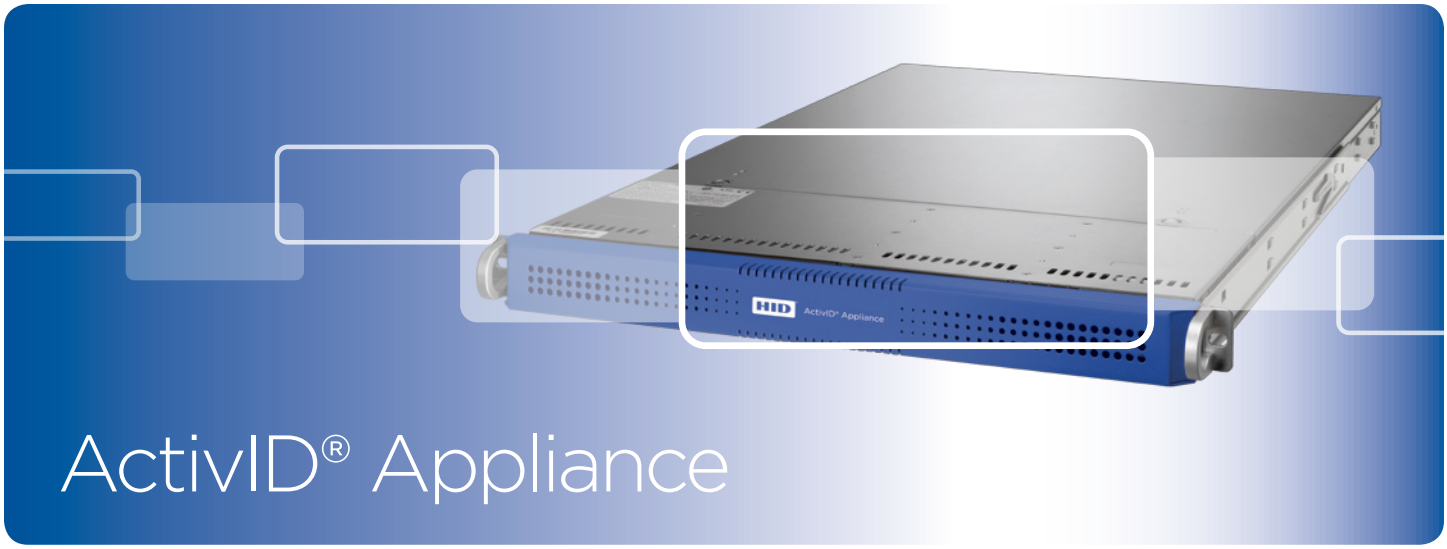
IDENTITY ASSURANCE SOLUTIONS



ActivID® Appliance

STRONG AND VERSATILE AUTHENTICATION APPLIANCE

- **Increase security** – Decreases risks with robust two-factor authentication which inhibits breaches.
- **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 and unobtrusive ActivID Threat Detection.
- **Lower cost** – Versatile, future-proof authentication platform reduces the cost of fulfillment and management.
- **Extend value** – Enables secure access from smartphone, iPad, laptop and PC to VPNs, web portals and cloud applications

ActivID Appliance includes a number of additional features that help organizations improve productivity:

- Secure access from laptops, browsers, tablets and smartphones with two-factor authentication
- Connect customers, employees, contractors and partners as needed for maximum business efficiency
- Simple and affordable for telecommuters and heavy smartphone users with Soft token Apps
- Broad range of hardware and software authentication methods provides options and price points to best meet business needs
- Protect cloud applications with the same authentication strength as used for internal applications
- Short message service (SMS) one-time passwords (OTP) ensure secure connectivity when tokens are not available or preferred
- ActivID Threat Detection transparently add layers of security and is only visible to end-users depending on the risk level of the transaction

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

Without sacrificing security, this solution ensures a convenient experience for end-users accessing sensitive resources from anywhere in the world, while using virtually any device, including their own smart phones, tablets or computers.

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

The ActivID Appliance enables organizations to tailor 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 and SMS Out-of-Band One-Time Password (OTP) options.

With the optional ActivID Threat Detection Service, the appliance can also transparently protect online transactions from a wide range of threats, including Trojan and man-in-the-browser (MitB) attacks.

Available as either a hardware appliance or a virtual appliance, the solution helps to reduce costs with easy installation, worry-free tokens that last up to eight years, and simple integration into an organization's existing network infrastructure.

FEATURES:

- Policy driven, 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.
- Security Domains provide strong segregation between different user populations.
- FIPS 140-2 HSM option to secure an organization's keys.
- 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).
- Organizations can generate their own seed files.
- 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

SPECIFICATIONS

Hardware Appliance
- 1U Chassis
- 650 W redundant PSU
- 2.0 GHz CPU Processor
- 8 GB RAM
- 4 x 1 TB Hot Swappable Hard Drive
- Hardware RAID 1 Mirroring
- UL, CUL, CSA, FCC, certification
- RoHS compliant
- Premium onsite hardware support option

Virtual Appliance Environment Requirements

Host
- Recent Intel® 32bit or 64bit; with min. 2.2 GHz, Dual Core
- 8GB of RAM
- 150GB of free HD space
- 2 network adapters if using dual node configuration
- VMware ESXi 5.0, ESXi 4.1+, or VMware Player 5.0.1, or VMware Workstation 8.x

VM Guest
- At least 4 GB of RAM (8 GB recommended)
- 2 CPUs/Cores
- 2 local network connections

Software Operating Environment
- Oracle Enterprise Linux – Hardened
- JBOSS 5.1.0.GA
- Embedded Oracle 11gR2 Standard
- Embedded Oracle GoldenGate

Hardware Security Module (optional)
- FIPS 140-2, level-3 certification
- Common Criteria EAL4+ certification
- FIPS 186-2 compliant random number generator

Built-in Authentication Methods	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 ActivID Threat Detection - Device Profiling & Risk Based authentication and browser based malware detection
External Authentication Methods	LDAP fallback & passthrough, RADIUS conditional routing
Authenticators	**Hardware Tokens** 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
	DisplayCard Tokens DisplayCard Token and Smart DisplayCard Token
	Software Tokens PC Soft Token, Mobile Soft Token (iOS, Android, Java, Blackberry, Windows Phone), Web Soft Token
User Repositories	**Database** Embedded Oracle 11g R2 Standard Edition with integrated fault tolerance **LDAP** Microsoft Active Directory, Oracle / Sun Java Directory, Novell eDirectory
Standards Supported	**Protocols** SAML v2, RADIUS Authentication and Authorization, Web Services (RMI & SOAP v1.1), LDAP v3, PSKC v1.0 (credential import), SNMP V3
	Cryptographic OATH event, time and challenge / response, 3DES / AES / RSA / ECC / SHA-2, FIPS 140-2 level 3 HSM (credential storage and data signing)
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

North America: +1 949 732 2000
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

hidglobal.com

ASSA ABLOY
An ASSA ABLOY Group brand

2013-02-15-identity-assurance-activid-appliance-ds-en