IDENTITY ASSURANCE SOLUTIONS

IDENTITY ASSURANCE SOLUTIONS
HID
ActivID AAA Server for Remote Access
ActivID AAA Server for Remote Access

ActivID AAA Server for Remote Access

ActivID AAA Server for Remote Access Benefits:

- **Increase Productivity:** Securely connect users from any location through simple authentication devices
- **Decrease Risk:** Securely connect users via robust two-factor authentication, to inhibits breaches
- **Reduce Costs:** Affordable server software supports long-lasting one-time password (OTP) tokens and cost-effective soft tokens
- **Accelerate Time-to-Benefit**: Easy deployment within existing IT environments, including directories, virtual private networks (VPNs), firewalls and remote access gateways
- Scale to hundreds of thousands of users
- Authenticate laptops, smartphones, PCs and tablets
- Leverage open standards for authentication protocols, directory protocols and OTP algorithms

STRONG AUTHENTICATION FOR REMOTE ACCESS AND BEYOND

HID Global's ActivID AAA Server for Remote Access for all your users, from 25 up to 200,000. AAA Server delivers flexible authentication, authorization and accounting (AAA) features, via an easy, best-in-class standards-based solution used by millions worldwide. AAA Server simultaneously strengthens security, reduces costs and enhances the user's experience.

AAA Server enables enterprises to secure and manage wireless local area networks (WLANs) and remote network access with a wide range of two-factor authentication devices, network access points and user stores. AAA Server supports the broad range of software and hardware tokens in the HID Global Identity Assurance portfolio.

To maximize usefulness, AAA Server supports essential protocols, such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+).

To minimize costs and administration, AAA Server fully leverages an organization's existing corporate directory. Enterprises can easily deploy distributed authentication that eliminates redundant administration load and offers centralized administration of user profiles.

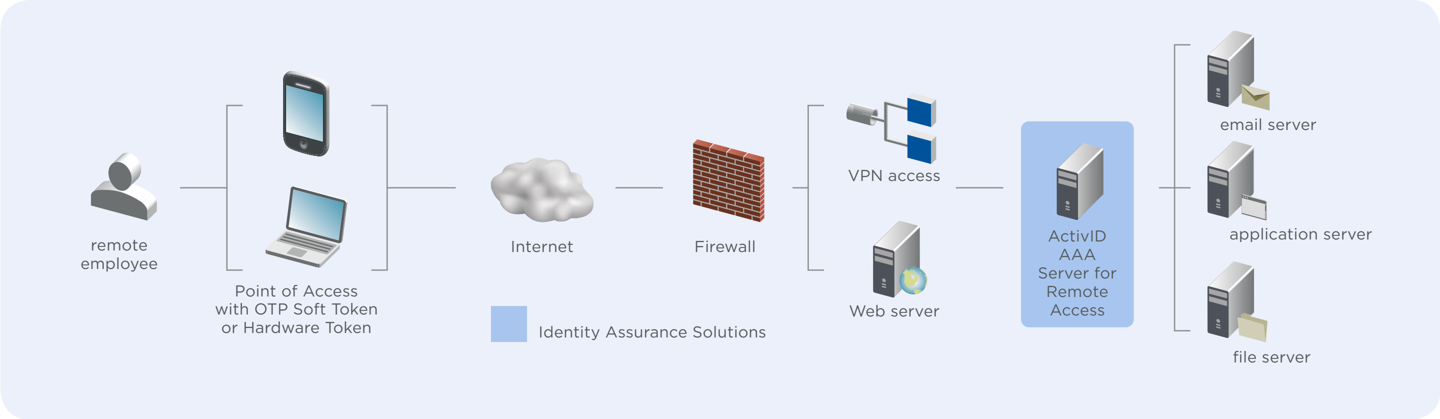
AAA Server also streamlines token issuance and reset with a user self-registration portal. This is especially helpful when remotely deploying soft tokens to a user's personal (bring your own device (BYOD)) smartphone or tablet.

To further enhance usability, when a user's OTP token is not present, AAA Server can send a short message service (SMS) text with a one-time password (OTP) to a user's pre-registered mobile phone.

Organizations seeking to deploy advanced fraud detection capabilities to secure cloud applications and multi-tenancy deployments should look at HID Global's ActivID® Appliance for best-in-class, versatile authentication.

SPECIFICATIONS

ActivID AAA Server for Remote Access: **How It Works**


remote employee
Point of Access with OTP Soft Token or Hardware Token
Internet
Firewall
VPN access
Web server
ActivID AAA Server for Remote Access
email server
application server
file server
Identity Assurance Solutions

System Requirements	**Operating Systems**
	Administration Console: Windows Server 2008, Windows Server 2008 R2 (32- and 64-bit where applicable), Windows Server 2012 R2, and Windows Server 2016 Authentication Server: Windows Server 2008, Windows Server 2008 R2 (32- and 64-bit where applicable), Windows Server 2012 R2, and Windows Server 2016
	Databases Microsoft SQL Server 2008 and 2008 R2 (Standard and Enterprise editions); SQL Server Express 2008 R2k, Microsoft SQL Server 2012 (32 and 64 bits), and Microsoft SQL Server 2014 SP1 Oracle 11g (Standard and Enterprise editions), Oracle 11g R2, and Oracle 12c
	Directories and Hardware (Minimum requirements) Microsoft Active Directory Server 2008 and 2008 R2, Microsoft Active Directory Server 2012 R2, and Microsoft Active Directory Server 2016. Oracle Directory Server Enterprise Edition 11.1.1. IBM® Tivoli® Directory Server 5.2
	Hardware No specific hardware requirements. (Hardware requirements should be the same as the OS where AAA is installed.)
User Authentication	**Methods** One-time password: Synchronous (3 variable-based ActivID-patented algorithm), OATH HOTP and TOTP One-time password: Synchronous + Server-based PIN (available for Mini Token) One-time password: Challenge / response SMS One-Time Password (+ an Activation Code) X.509 certificate (EAP-TLS) Static password LDAP password Routing to external RADIUS authentication server
	Authentication Devices Hardware Tokens: Token, Pocket Token, Keychain Token, Mini Token (AE, AT, OE and OT), Desktop Token Smart Cards and USB Keys: Smart Card, ActivKey SIM, ActivKey Display, DisplayCard – together with ActivClient middleware and optionally ActivID Credential Management System ActivID Soft Tokens: Mobile Soft Token (Android, BlackBerry, iPhone, Java Phone, Windows Mobile), PC Soft Token, Web Soft Token
Standards Supported	**Protocols** RADIUS RFC 2865, 2866, and 2869 TACACS+ RADIUS support for EAP: RFC 3579 and 3748 EAP-TLS RFC 2716 IEEE 802.1X (EAP-TLS, PEAP-MSCHAP v2, PEAP-GTC)
	Cryptographic DES, 3DES ANSI X9.9 (challenge / response) ANSI X9.17 (key management) Retail Financial Services Symmetric Key Management ANSI X9.52 One-Time-Password: OATH HOTP and TOTP
Supported Applications	VPN, Dialup-up, Firewalls and Wireless LAN products compatible with RADIUS or TACACS+, e.g. from Avential, Check Point, Cisco, Juniper, Microsoft, Nortel, Symantec Web servers (Microsoft IIS, Sun One) Citrix XenApp Server Microsoft Terminal Server Microsoft Outlook Web Access / Web App Any application supporting RADIUS or TACACS+ for authentication
Administration	Capability to define authentication, authorization, and accounting profiles Device management
Auditing, Accounting, and Reporting	Capability to consolidate, view, and delete audit logs RADIUS accounting (RFC 2866)

North America: +1 512 776 9000
Toll Free: 1 800 237 7769
Europe, Middle East, Africa: +49 6123 791 0
Asia Pacific: +852 3160 9800
Latin America: +52 55 5081 1650

hidglobal.com

ASSA ABLOY
An ASSA ABLOY Group brand