



# 4TRESS™ AAA Server for Remote Access

### 4TRESS AAA Server Benefits:

- **Increase Productivity:** Securely connect users from any location through simple authentication devices
- **Decrease Risk:** Securely connect users via robust two-factor authentication, to inhibit 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 4TRESS 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+).

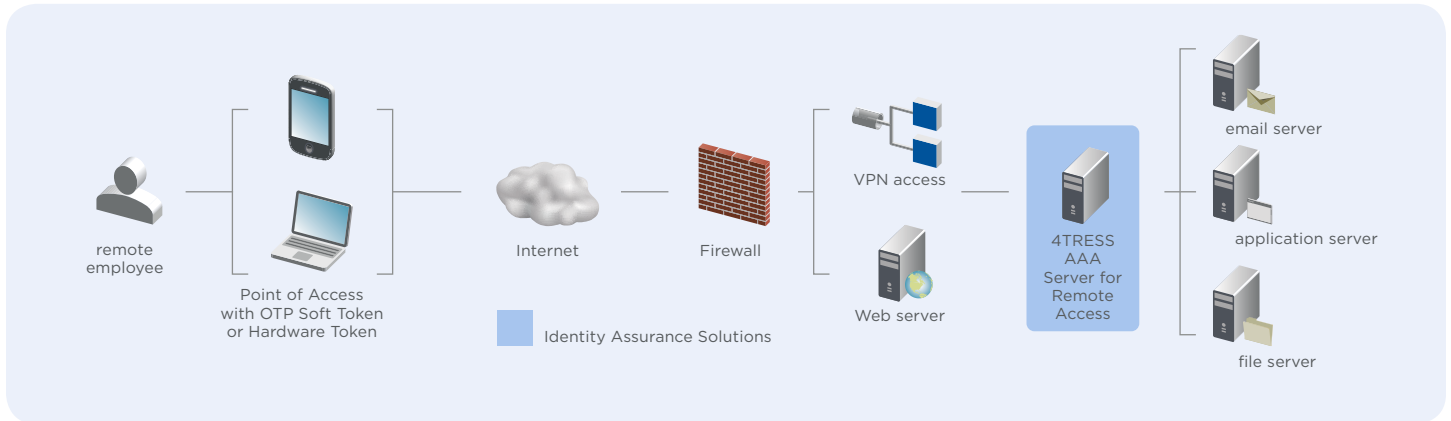
To minimize costs and administration, AAA Server fully leverages an organization's existing corporate directory. Enterprises can easily deploy distributed authentication that eliminates redundant administration load and offers centralized administration of user profiles.

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.

4TRESS for Remote Access: **How It Works**



System Requirements	Operating Systems	
	Administration Console: Microsoft® Windows XP Pro, Windows Vista, Windows 7, Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 (32- and 64-bit where applicable) Authentication Server: Microsoft Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2 (32- and 64-bit where applicable)	
	<b>Databases</b> Microsoft SQL Server 2000, 2005, 2008 and 2008 R2 (Standard and Enterprise editions); SQL Server Express 2005 and 2008 R2 Oracle 8.1.7.4, 9i, 10g and 11g (Standard and Enterprise editions)	
	<b>Directories and Hardware (Minimum requirements)</b> Microsoft Active Directory Server 2003, 2003 R2, 2008 and 2008 R2 Sun™ Java System Directory Server 5.2, 6.1 and 6.3	
	<b>Hardware</b> Intel® Pentium® III 650 Mhz 128 MB RAM, 4 GB hard disk	
User Authentication	<b>Methods</b> 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	
	<b>Authentication Devices</b> 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	<b>Protocols</b> 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)	<b>Cryptographic</b> 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: +1 949 732 2000  
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

**ASSA ABLOY**  
An ASSA ABLOY Group brand

© 2013 HID Global Corporation/ASSA ABLOY AB. All rights reserved. HID, HID Global, the HID Blue Brick logo, the Chain Design, ActivID, ActivClient and 4TRESS 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.