

Actividentity 4TRESS™ AAA Server

➤ Scalable strong authentication solution

Secure Remote Access and WLAN with One-time passwords

4TRESS™ AAA Server is a strong scalable RADIUS and TACACS+ compliant server. Offering full Authentication, Authorization, and Accounting services, 4TRESS AAA Server enables enterprises to secure and manage WLAN and remote network access with two-factor authentication. It is the only one-time password authentication server on the market that features native WLAN security and fully leverages your existing corporate directory.

Key features

Enhanced security

- Allows local initialization of tokens and smart cards, ensuring that keys are securely deployed.
- One-time passwords are generated using a patented algorithm based on three variables: time, an event counter and a cryptographic key that is updated for each authentication. This provides a higher level of security than other one-time password solutions based on one or two variables only.

- Integrated WLAN security Wireless Protected Access (WPA) 802.1x authentication.

Easy implementation and administration

- Supports LDAP directories and SQL compatible databases, therefore requiring no proprietary database—enabling centralized administration with distributed authentication.
- Designed for easy installation and deployment.

Secure dial-up and VPN

- Supports all leading network access servers, routers and IPSEC or SSL-based VPNs via the RADIUS and TACACS+ standards.

Secure web access

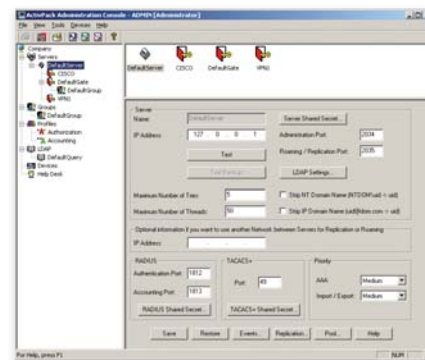
- Provides strong one-time password authentication for any website running on IIS or Sun® Java™ System web servers, as well as Microsoft Outlook® Web Access.

Secure wireless LAN

- Enables Wi-Fi authentication with support for EAP (Extensible Authentication Protocol) compatible with Wi-Fi Protected Access (WPA and WPA2).

Secure terminal services

- Secure login to Citrix® Presentation Server™ - Web Interface.



Benefits

Compelling ROI

Provides a lower total cost of ownership than the competition—even if existing two-factor remote access technology is in place. LDAP-centric integration eliminates dual administration.

Smooth bridge and migration

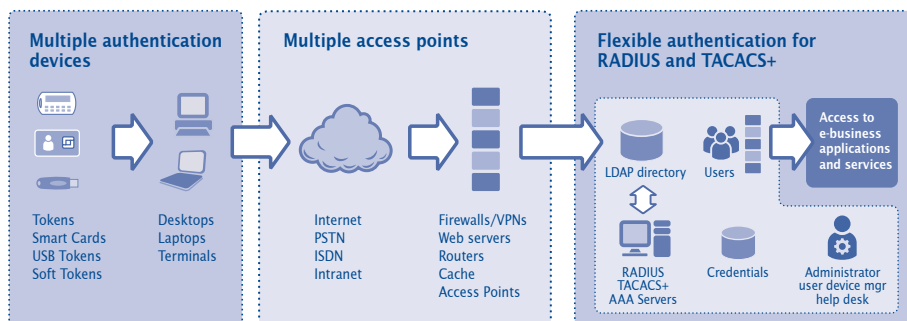
Supports all current and future authentication needs. Allows enterprises to deploy a mixed environment of static passwords, tokens, soft tokens, USB tokens, and smart cards to allow migration from a single function token solution to a multi-application smart card-based environment.

Ease of use

Brings the ATM experience to network computing, simplifying the user experience with the universally accepted PIN entry method. PIN entry allows access to multiple authentication credentials on a single smart card device.



4TRESS AAA Server architecture for remote access



4TRESS AAA Server is an enterprise solution for verifying user authentication requests and instantly enforcing security policies across distributed sites worldwide.

4TRESS AAA Server components

- Administration Console
- Authentication Server (RADIUS, TACACS+, IEEE 802.1x)
- Optional Components
 - Web help desk & self service portal
 - Web access agent (IIS & Sun One)
 - Citrix® Presentation Server™ – Web Interface agent
 - Novell® NMAST™ agent
 - Realm Proxy
- Interfaces and APIs
 - Help desk and self service interface web API (SOAP/HTTPs)
 - Remote Authentication API (ANSI C)

Administration services

- Administrator
 - Manage authentication server parameters and access gates
 - Define authorization, authentication and accounting profiles
 - Define authorization profiles based on conditional statement
- Audit manager
 - Consolidate, view, and delete auditing logs
- Device manager
 - Create, delete, and initialize devices
 - Assignment of devices
- Help desk
 - Lock, unlock, and resynchronize personal devices
 - Activate, deactivate emergency access
- Self service portal
 - Unlock and resynchronize
 - Report lost, stolen devices

Security services

- EAP-TLS, PEAP-GTC, PEAP-MSCHAPv2
- Authenticate users from routers, firewalls, APs, VPNs, or Web servers
- Encryption of:
 - Administration database
 - Remote administration sessions
 - Device to server authentications
 - Authentication server exports
 - User PIN, credentials, and keys
- Import/export secret key management

Authentication options

- One-time Password, Static Password, LDAP Password, X509 Certificate, Short Message Service (SMS)
- Hardware tokens
 - ActivIdentity Token
 - ActivIdentity Keychain Token
 - ActivIdentity Mini Token
 - ActivIdentity Desktop Token
 - ActivIdentity Pocket Token
- ActivIdentity Soft Token for PC, JavaPhone™, Palm® and PocketPC
- ActivKey™ USB tokens
- ActivIdentity Smart Cards

Compliance with industry standards

- Data Encryption Standard: 3DES
- Challenge/Response: ANSI X9.9
- Key Management: ANSI X9.17
- Radius RFC 2865, 2866 and 2869
- RADIUS support for EAP: RFC 3579, 3748, EAP-TLS RFC 2716

Compatibility

- Any RADIUS and TACACS+ server or client (Firewalls, VPNs, Routers, 802.1x compliant Access Points)
- Check Point FireWall-1®
- Check Point VPN-1 SecuRemote™
- Cisco® Systems Secure PIX® Firewall
- Cisco Systems Secure VPN
- Cisco 802.1x clients
- Citrix Presentation Server Web Interface
- Citrix Access Gateway™
- Funk Odyssey 802.1x client
- Juniper® Firewall and VPN
- Microsoft® 802.1x clients
- Microsoft IIS web server
- Microsoft RAS client
- Microsoft Outlook Web Access
- Nortel Networks™ Contivity
- Novell Modular Authentication Service (NMA)
- Microsoft SQL Server, Microsoft Desktop Engine, Oracle® databases
- Sun Java™ System Web server
- Directory Services: Critical Path Directory Server, IBM® Tivoli® Directory Server, Microsoft Active Directory, Novell eDirectory™, Sun Java System Directory Server
- Leading reporting tools server

System requirements administration console

- Intel® Pentium® III 650MHz
- 128 MB RAM, 100 MB hard disk
- Microsoft Windows® 2000 (SP4), Windows XP Pro (SP1) or Windows Server 2003 SP1
- ODBC compatible database

Authentication server

- Intel Pentium III 650 MHz
- 128 MB RAM, 4 GB hard disk
- Windows 2000(SP4) or Windows 2003
- ODBC compatible database

Web help desk & self service portal

- Internet Explorer 5.5 SP2 or later

Web access agents

- Sun Java™ System Web Server 6.0, iPlanet Web Server 6.0
- Microsoft IIS 5.0, 6.0/Windows 2000/2003
- Internet Explorer 5.5 SP2 or later

ActivIdentity related documents

- ActivIdentity Tokens data sheet
- ActivKey™ data sheet
- ActivClient® data sheet
- Strong Authentication solution brief
- Smart Employee ID solution brief
- Device and Credential Management solution brief



To find out more about
 ActivIdentity products, visit
 our website

www.actividentity.com

Americas +1 (510) 574 0100

US Federal +1 (571) 522 1000

Europe +33 (0) 1 42 04 84 00

Asia Pacific +61 (0) 2 6208 4888

Email info@actividentity.com

ActivIdentity®