

# ActivIdentity 4TRESS™ Authentication Appliance For Enterprises



## AT-A-GLANCE:

### The ActivIdentity 4TRESS Authentication Appliance benefits include:

- Increase productivity: securely connect from any location through a variety of devices and authentication methods
- Decrease risk: securely connect users via robust two-factor authentication, which inhibits breaches
- Reduce costs: by using a versatile, future-proof authentication platform
- Improve control: by employing an open and fully interoperable OATH-standards-based authentication and by extending the choice of authentication devices
- Extend value: secure smart phones, iPad, laptop & PC access to VPNs, web portals and cloud applications

## Strong Authentication for Remote Access and Beyond

ActivIdentity's 4TRESS™ Authentication Appliance provides versatile strong authentication for all employees, accessing a wide range of applications, including VPN Remote Access, Terminal Services, and Private and Public Clouds.

Through a single appliance, ActivIdentity supports a multitude of authentication methods to protect your data, network and reputation assets. 4TRESS allows you to tailor authentication methods to the needs of specific groups of users, providing each the right balance of security, cost and convenience to meet your business objectives.

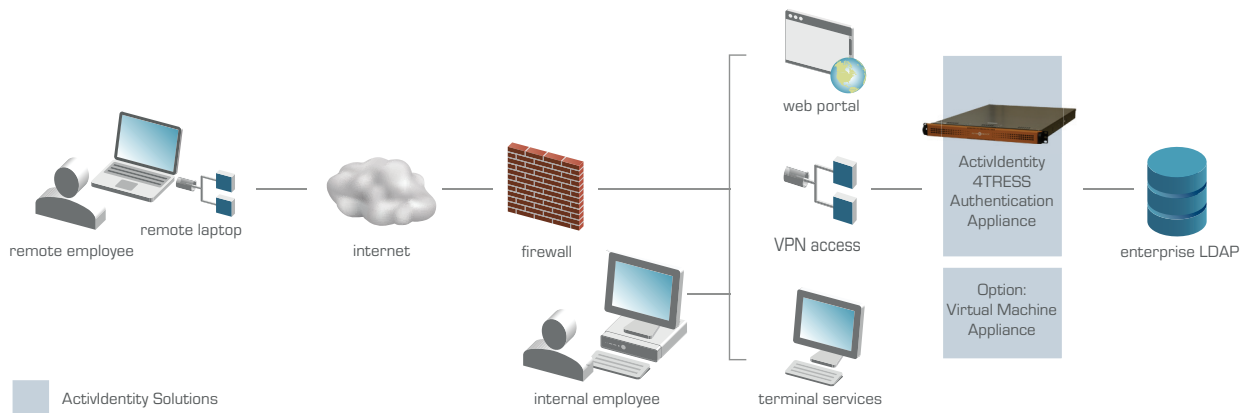
4TRESS increases productivity by securely authenticating users remotely via their preferred smartphone, browser or computer through a variety of devices and authentication methods. The 4TRESS Authentication Appliance supports the broadest choice of authentication methods, from strong passwords though to certificate-based authentication, including two-factor OATH-standards-based hardware tokens, soft tokens, and SMS Out-of-Band One-Time Password (OTP) options.

The 4TRESS Authentication Appliance reduces costs with easy installation, worry-free tokens that last up to eight years, and simple integration into your existing network infrastructure.

### ActivIdentity 4TRESS™ Authentication Appliance

Virtual Appliance Available





**“We wanted the ability to rapidly deploy authentication methods to meet the market need without changing the infrastructure and technology each time and 4TRESS allows us to do this.”**

**Maud Brunswick**  
Project manager  
@ BNP Paribas

### Improve productivity

- Securely access from laptops, browsers, and smartphones with two-factor authentication
- Connect employees, contractors and partners as needed for maximum business efficiency
- Simple and affordable enough for telecommuters, day extenders, road warriors, and heavy-smartphone users
- Standards-based OATH tokens provide the broadest range of features, suppliers and price points to best meet business needs
- Soft tokens allow more convenient and economical strong authentication of remote workers
- Soft tokens don't require extra devices or rekeying. They are easy to distribute, less expensive and can be recycled as employees change
- SMS OTP ensures secure connectivity if tokens are not available or not preferred

### Easy migration

- Appliance simplifies and streamlines deployment
- Works concurrently with legacy authentication servers for graceful and efficient migration, which maximizes ROI of old tokens, and ensures lowest-risk migration

- Ability to leverage existing user directories eliminates the need for user migration during deployment
- Able to link to multiple LDAPs with a single front end

### Decrease risk

- Option to generate your own seed files
- Using PIN + token enhances security and provides the confidence to connect with all forms of digital connections
- Multi-factor authentication limits impact of some forms of malware
- Strong authentication improves regulatory compliance and policy adherence
- Three-factor authentication is provided via time, event counter seed key, and PIN usage with algorithm
- Supports the broadest range of OTP algorithms based on OATH open standards including time-based, event-based, and proprietary time+event-based algorithms for maximum security, utility and value
- Tokens auto-synchronize, which improves reliability, security, and reduces support calls
- Integrates seamlessly with full suite of credential management, middleware, smart card, single sign-on, mobility, and physical access control offerings
- Integrates with Active Directory and most standard LDAP to match the scalability and availability of your network



## Versatile authentication reduces costs

- Broad range of authentication methods
  - ActivIdentity OTP tokens (Mini Token, Pocket Token, Token One, Desktop Token)
  - ActivIdentity Display Card
  - 3rd party tokens compliant with the Oath OTP standards (HOTP / TOTP)
  - Vasco Digipass tokens
  - ActivIdentity Mobile, PC, Web tokens
  - DeviceID
  - Strong passwords (full and partial)
  - Security questions & answers (full and partial)
  - Certificate-based authentication (PKI)
  - Smart cards running the ActivIdentity OTP applet
  - Out-of-band SMS (password or verification code)
  - Out-of-band Email (password or verification code)
  - Temporary activation codes
  - LDAP passwords
  - RADIUS authentication

- Virtual appliance option
- Compliant with the OATH industry standard, eliminating vendor “lock-in”
- Competitively sourced, standards-based OATH tokens ensure right features and best value
- Tokens can last up to eight years, 2x to 3x longer than other solutions, dramatically lowering token replacement and redeployment costs
- Soft tokens deploy more efficiently



## Improve Control

- 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
- FIPS 140-2 HSM option to secure your keys

**“Almost 50% of data breaches exploit stolen or weak credentials.”**

Verizon Business Data Breach Investigations Report, 2010

## Strong Authentication for Cloud Applications: How It Works



## Technical Specifications

ActivIdentity 4TRESS Authentication Server		ActivIdentity 4TRESS Authentication FT2011	
<b>Built-in Authentication Methods</b>	<ul style="list-style-type: none"> <li>- One-time password: Synchronous (ActivIdentity patented algorithm)</li> <li>- One-time password: Challenge / response</li> <li>- One-time password: OATH HOTP Event, TOTP Time-based, and OCRA challenge / response</li> <li>- Oath transaction signing (OCRA)</li> <li>- Smart Card PKI / X.509 certificate</li> <li>- Emergency full and partial strong Static Password &amp; Security Questions</li> <li>- Out-Of-Band One-Time Password or Transaction Verification code sent via SMS or Email</li> <li>- Device ID - Web Browser Registration</li> <li>- 4TRESS Fraud Detection - Device Profiling &amp; Risk Based authentication</li> </ul>	<b>Appliance</b>	<b>Chassis Form Factor</b> <ul style="list-style-type: none"> <li>- 1U Chassis</li> <li>- 650 W redundant PSU</li> <li>- DVD-ROM</li> </ul>
<b>External or Third-Party Authentication Methods</b>	<ul style="list-style-type: none"> <li>- LDAP fallback &amp; passthrough</li> <li>- RADIUS conditional routing</li> </ul>	<b>Processor Type</b>	- 2.0 GHz CPU
<b>Authenticators</b>	<b>Hardware Tokens</b> <ul style="list-style-type: none"> <li>- ActivIdentity OTP Token VL</li> <li>- ActivIdentity KeyChain OTP Token</li> <li>- ActivIdentity Desktop OTP Token</li> <li>- ActivIdentity Pocket OTP Token</li> <li>- ActivIdentity Mini OTP Token</li> <li>- Any OATH compliant event, time or challenge / response-based hardware token</li> </ul> <b>DisplayCard Tokens</b> <ul style="list-style-type: none"> <li>- ActivIdentity DisplayCard Token</li> </ul> <b>Software Tokens</b> <ul style="list-style-type: none"> <li>- ActivIdentity PC Soft Token</li> <li>- ActivIdentity Mobile Soft Token (iPhone, Android, Java, Blackberry)</li> <li>- ActivIdentity Web Soft Token</li> </ul>	<b>Memory</b>	- 8 GB RAM
<b>User Repositories</b>	<b>Database</b> <ul style="list-style-type: none"> <li>- Embedded Oracle 11g R2 Standard Edition with integrated fault tolerance</li> </ul> <b>LDAP</b> <ul style="list-style-type: none"> <li>- Microsoft Active Directory</li> <li>- Oracle / Sun Java Directory</li> <li>- Novell eDirectory</li> </ul>	<b>Drive</b>	<ul style="list-style-type: none"> <li>- 4 x 250 GB Hard Drive</li> <li>- Hardware RAID 1 Mirroring</li> </ul>
<b>Standards Supported</b>	<b>Protocols</b> <ul style="list-style-type: none"> <li>- SAML v2</li> <li>- RADIUS Authentication and Authorization</li> <li>- Web Services (RMI &amp; SOAP v1.1)</li> <li>- LDAP v3</li> <li>- PSKC v1.0 (credential import)</li> </ul> <b>Cryptographic</b> <ul style="list-style-type: none"> <li>- OATH event, time and challenge / response-based</li> <li>- 3DES / AES / RSA / ECC / SHA-2</li> <li>- FIPS 140-2 level 3 HSM (credential storage and data signing)</li> </ul>	<b>Regulatory</b>	<ul style="list-style-type: none"> <li>- UL, CUL, CSA, FCC, certification</li> <li>- RoHS compliant</li> </ul>
<b>Help Desk and Self Service</b>	<ul style="list-style-type: none"> <li>- Web-based help desk</li> <li>- Localizable &amp; U.S. Section 508 compliant</li> </ul>	<b>Virtual Appliance Environment Requirements</b>	<b>Host</b> <ul style="list-style-type: none"> <li>- Recent Intel® 32bit or 64bit; with min. 2.2 Ghz, Dual Core</li> <li>- 4GB of RAM (6GB or more recommended)</li> <li>- 150GB of free HD space</li> <li>- VMware ESXi 7.1, or VMware-player 3.1[VMware-player-3.1.4-385536.exe], or VMware-workstation 7.1[VMware-workstation-full-7.1.4-385536.exe]*</li> </ul> <b>VM Guest</b> <ul style="list-style-type: none"> <li>- At least 2.5GB of RAM (4GB recommended)</li> <li>- 2 CPUs/Cores</li> <li>- 2 local network connection</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>- Device and Credential management</li> <li>- Authentication Policy management</li> <li>- User and Permission management</li> </ul>	<b>Software Operating Environment</b>	<b>Operating System</b> <ul style="list-style-type: none"> <li>- Oracle Enterprise Linux – Hardened</li> </ul> <b>Application Server</b> <ul style="list-style-type: none"> <li>- JBOSS 4.2.3 GA</li> </ul> <b>Database</b> <ul style="list-style-type: none"> <li>- Oracle 11gR2 Standard Edition Embedded with fault tolerance</li> </ul>
<b>Auditing, Accounting and Reporting</b>	<ul style="list-style-type: none"> <li>- Digitally signed &amp; sequenced tamper-evident audit log</li> <li>- Audit log queries</li> <li>- Published audit schema</li> </ul>	<b>Hardware Security Module (optional)</b>	<b>Vendor</b> <ul style="list-style-type: none"> <li>- RealSec Crypto</li> </ul> <b>Processor</b> <ul style="list-style-type: none"> <li>- ARM7TDMI 50 MHz RISC processor</li> </ul> <b>Certifications</b> <ul style="list-style-type: none"> <li>- FIPS 140-2, level-3 certification</li> <li>- Common Criteria EAL4+</li> </ul> <b>Cryptographic – Random</b> <ul style="list-style-type: none"> <li>- FIPS 186-2 compliant random number generator</li> </ul> <b>Cryptographic – Symmetric</b> <ul style="list-style-type: none"> <li>- AES, DES, Triple DES (double and triple length cipher);</li> <li>- SAFER (64 and 128 bits, K and SK modes)</li> <li>- Throughput: 320-600 MBs</li> </ul> <b>Cryptographic – Asymmetric</b> <ul style="list-style-type: none"> <li>- RSA 1024, RSA 2048</li> <li>- RSA 4096 &amp; ECC ready</li> <li>- Throughput: 337-7240 exp/s</li> </ul> <b>Cryptographic – Hashing</b> <ul style="list-style-type: none"> <li>- Hash functions: MD5, SHA-1, RIPEMD (128 and 160 bits)</li> </ul>

\*Note for VM conversion, we recommend VMware-converter: VMware-converter-all-4.3.0-292238.exe



## 4TRESS Fraud Detection

**Americas** +1 510.574.0100

**US Federal** +1 510.574.0100

**Europe** +33 (0) 1.42.04.84.00

**Asia Pacific** +61 (0) 2.6208.4888

**Email** info@actividentity.com

**Web** www.actividentity.com



**ASSA ABLOY**  
An ASSA ABLOY Group brand

## About ActivIdentity

ActivIdentity Corporation, a global leader in identity assurance, enables customers to prove and establish trust in a person's identity when accessing resources on the network. The business's strong authentication and smart card solutions are relied upon by more agencies, including the U.S. Department of Defense, than any other provider, and has issued more than 100 million credentials to enterprise, government and commerce customers. ActivIdentity is headquartered in Silicon Valley, California. ActivIdentity is part of HID Global, an ASSA ABLOY Group brand. For more information, visit [www.actividentity.com](http://www.actividentity.com)

Follow Us On:

Copyright © 2010 ActivIdentity. All rights reserved. ActivIdentity®, ActivID, ActivIdentity SecureLogin, ActivClient, and 4TRESS are trademarks of ActivIdentity. All other trademarks, trade names, service marks, service names, and images mentioned and / or used herein belong to their respective owners.