DS

DATA SHEET

ActivIdentity 4TRESS

Versatile authentication platforms for secure access

ActivIdentity 4TRESS Benefits

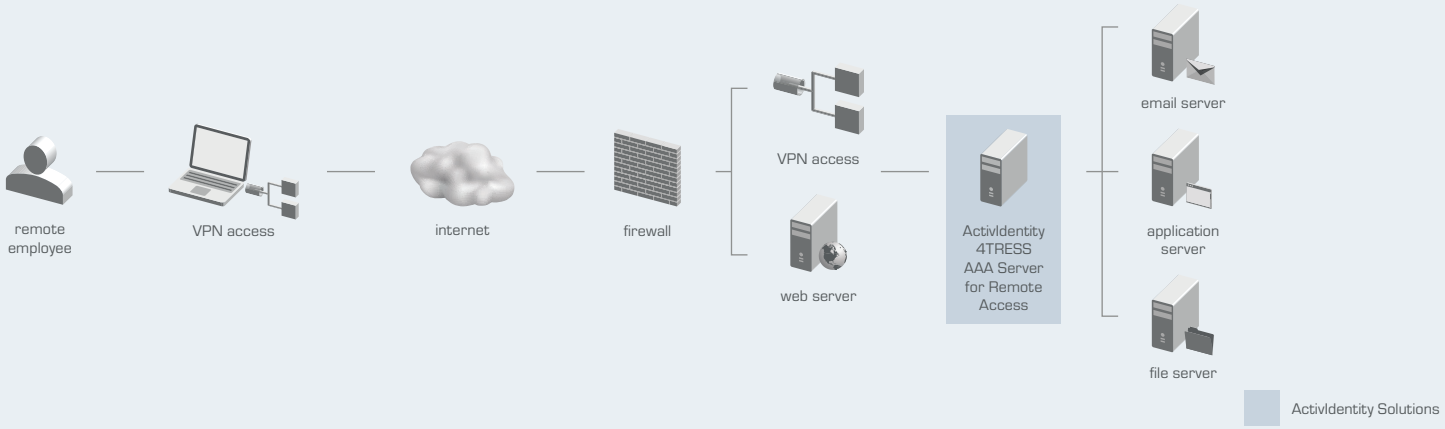
- Cost-effective multi-factor authentication, which eliminates the vulnerabilities associated with static passwords
- Broad support of authentication devices and authentication methods that provide user convenience and address a variety of risk levels for organizations
- An open standards-based platform that seamlessly integrates into any existing computing environment
- Support for compliance with industry and government regulations covering multi-factor authentication, authorization, and auditing

The ActivIdentity 4TRESS™ suite of authentication products provides a complete, versatile authentication solution for organizations seeking to extend access control beyond traditional user name and password mechanisms. Versatile authentication solutions add strategic value by giving organizations the flexibility to meet current and future needs for a range of deployment, user, device, and service-channel options. The ActivIdentity 4TRESS authentication solutions also enable organizations to centralize management of heterogeneous, siloed authentication instances – either en masse or over time. Using the ActivIdentity 4TRESS suite of products, organizations can meet a variety of access control use cases while minimizing the cost and complexity of deploying and managing disparate policies and credential life cycles.

ActivIdentity 4TRESS authentication solutions include the following features and capabilities:

- A broad choice of authenticators based on open standards (e.g., Initiative for Open AuTHentication [OATH]; Europay, MasterCard, and Visa [EMV]; and public key infrastructure [PKI] standards) as well as authentication mechanisms based on proprietary authentication schemes
- A flexible set of deployment options that gives enterprises the scale and performance they require
- Centralized authentication, authorization, and audit capabilities to strengthen compliance and streamline reporting
- Device and credential life cycle management

ACTIVIDENTITY™



ActivIdentity 4TRESS AAA Server for Remote Access Benefits

- Easy installation and deployment within existing IT environments, including directories, certificate authorities, virtual private networks (VPNs), firewalls, and remote access gateways
- Migration of legacy authenticators over time and with no disruption to users
- Based on open standards for authentication protocols, directory protocols, and one-time password (OTP) algorithms
- Scalable to hundreds of thousands of users

Third-party Interoperability

- Microsoft
- Cisco
- Juniper
- OATH
- VISA
- MasterCard

The ActivIdentity 4TRESS suite includes the ActivIdentity 4TRESS™ AAA Server for Remote Access and the ActivIdentity 4TRESS Authentication Server. In addition, ActivIdentity offers a broad range of hardware tokens, smart cards, and soft tokens. The ActivIdentity 4TRESS offering also includes a software development kit for systems integrators and independent software vendors.

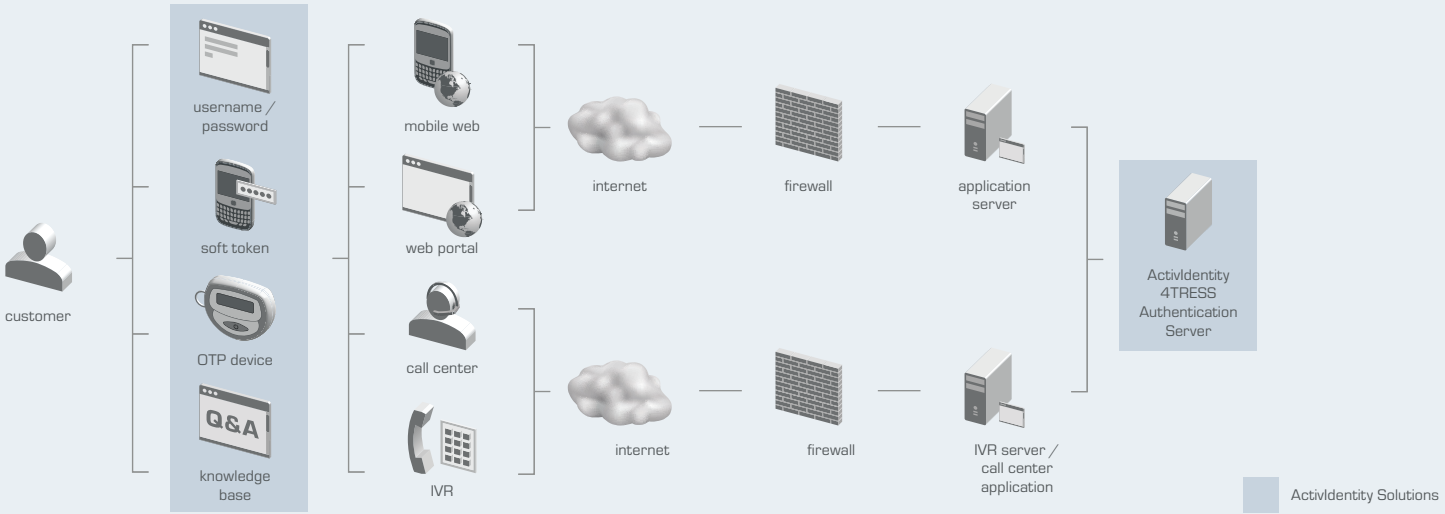
ActivIdentity 4TRESS AAA Server for Remote Access

The ActivIdentity 4TRESS AAA Server for Remote Access provides flexible authentication, authorization, and accounting (AAA) features using open standards-based protocols such as Remote Authentication Dial-In User Service (RADIUS) and Terminal Access Controller Access-Control System Plus (TACACS+). As a best-in-class product for securing access to enterprise networks, ActivIdentity 4TRESS AAA Server for Remote Access supports a wide range of authentication devices, hard and soft authentication mechanisms, network access points, and user stores.

The ActivIdentity 4TRESS AAA Server for Remote Access fully leverages an organization's corporate directory, allowing organizations to easily deploy distributed authentication while eliminating redundant administration and maintaining centralized administration of user profiles.

When the ActivIdentity 4TRESS AAA Server for Remote Access is deployed with the ActivIdentity ActivClient™ security software, organizations can use smart cards for both strong authentication to the corporate network and physical access to corporate facilities. The ActivIdentity ActivID™ Card Management System adds a critical management layer for large smart card deployments. It supports post-issuance of smart card applications and credentials, self-service operations for users, and a robust set of administration capabilities (including suspension and revocation).

ActivIdentity 4TRESS™ Authentication Server: How It Works



ActivIdentity 4TRESS Authentication Server

The ActivIdentity 4TRESS Authentication Server allows customer-facing organizations to use a consistent authentication model across their electronic service channels. The ActivIdentity 4TRESS Authentication Server platform is designed to maximize authentication versatility, accommodate multiple business units, and scale to millions of users. The platform segregates data and administration control so that large organizations can leverage the same instance across business lines, and service providers can use the platform to add authentication services in a multi-tenant environment.

The ActivIdentity 4TRESS Authentication Server supports a layered approach that enables organizations to tailor the authentication method (e.g., static password, knowledge-based data, OTP, or PKI) and authenticator (e.g., hardware token, soft token, or smart card) to specific user groups and risk levels. By providing an open and extensible framework to add new authentication methods and credential types, the ActivIdentity 4TRESS Authentication Server lets organizations respond quickly to new online attacks, evolving business requirements, and changing user needs.

ActivIdentity 4TRESS Authentication Server Benefits

- Broad range of authentication methods and devices based on open standards (e.g., OATH, EMV, and PKI)
- Comprehensive management tools providing complete life cycle management for user credentials, soft tokens, and devices
- Centralized and tamper-evident audit logs for tracking transactions across channels, improving security, and simplifying compliance
- Highly scalable deployment architecture that supports multiple application servers and platforms
- Extensible framework to easily add third-party authentication methods

Technical Specifications

	ActivIdentity 4TRESS Authentication Server 4.1	ActivIdentity 4TRESS AAA Server for Remote Access 6.6
System Requirements - Operating systems - Hardware - User stores - Application servers - Hardware security modules	**Operating Systems** - Sun Solaris™ 9 and 10 - IBM AIX 5.3 - Redhat® Enterprise Linux® 5 **Databases** - Oracle® 10g and Oracle 10 Express **Application Servers** - IBM WebSphere® Application Server v6.0.x and 6.1.x - JBOSS® Application Server 4.2.x **Hardware** - Sun SPARC® (Sun Fire 280 and 240) - IBM pSeries System p5 Servers - Intel x64 PC - Hardware Security Module (HSM) · nCipher® HSM - nShield - payShield for EMV - netHSM · SafeNet® HSM - ProtectServer External	**Operating Systems** - Administration Console - Microsoft Windows® 2000 Professional SP3 / SP4 - Microsoft Windows XP Pro SP1 / SP1a / SP2 - Microsoft Windows Server 2003 SP1 / R2 and SP2 - Microsoft Windows Vista (32-bit only) - Authentication Server - Microsoft Windows 2000 Server SP4 (32- bit) - Microsoft Windows Server 2003 SP1 / R2 (32-bit) and SP2 - Microsoft Windows Server 2008 (32-bit) and SP2 **Databases** - Microsoft® SQL Server 2000 SP3 / SP3a / SP4, 2005 (Standard and Enterprise editions) - Microsoft SQL Server 2005 Express edition (default setting) - Oracle 9i and 10g (Standard and Enterprise editions) **Directories** - Microsoft® Active Directory Server 2000, 2003 - Sun™ Java System Directory Server 5.2, 6.2 (on Windows 2000 / 2003) - Critical Path Directory Server 4.2 (on Windows 2000 and Solaris 8) - Novell® eDirectory 8.7.3, 8.8 - IBM Tivoli Directory Server 5.2 **Hardware (Minimum requirements)** - Intel® Pentium® III 650 Mhz - 128 MB RAM, 4 GB hard disk
Built-in Authentication Methods	- One-time password: Synchronous (ActivIdentity-patented algorithm) - One-time password: Challenge / response - One-time password: OATH event, time-based, and challenge /response - One-time password: EMV CAP / DPA - X.509 certificate - Static and partial static password - Question and answer data	- One-time password: Synchronous (ActivIdentity-patented algorithm) - One-time password: Challenge / response - One-time password: OATH event and time-based - SMS one-time password - X.509 certificate - Static password - LDAP password
External or Third-Party Authentication Methods	- Static password and one-time password (Any RADIUS-compliant authentication server via proxy)	- Static password and one-time password (ODBC / JDBC-compliant database, remote RADIUS server, or LDAP v3 directory)
Standards Supported	**Protocols** - RMI, SOAP v1.1 - PSKC v1.1 (credential import) **Cryptographic** - EMV CAP / DPA - 3DES / AES - FIPS 140-2 level 3 (credential storage and data signing)	**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)
Help Desk and Self Service	- Web-based help desk and self service	- Web-based help desk and self service (optional)
Administration	- Device and credential management - User and permission management - Password management	- Capability to define authentication, authorization, and accounting profiles - Device management
Auditing, Accounting, and Reporting	- Digitally signed tamper-evident log - Audit log queries, Published schema - Crystal Reports®	- Capability to consolidate, view, and delete audit logs - RADIUS accounting (RFC 2866)
Compatibility with other ActivIdentity software products		- ActivIdentity ActivClient™ product family - ActivIdentity ActivID™ Credential Management System

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
Web www.actividentity.com

About ActivIdentity

ActivIdentity Corporation (NASDAQ: ACTI) is a global leader in strong authentication and credential management, providing solutions to confidently establish a person's identity when interacting digitally. For more than two decades the company's experience has been leveraged by security-minded organizations in large-scale deployments such as the U.S. Department of Defense, Nissan, and Saudi Aramco. The company's customers have issued more than 100 million credentials, securing the holder's digital identity.

ACTIVIDENTITY™