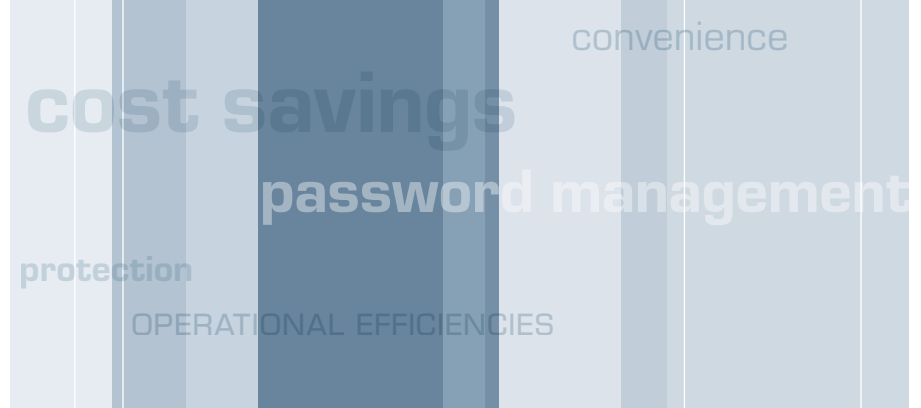


# ActivIdentity SecureLogin Single Sign-On

Market-leading password management solution for secure, convenient access to resources



## ActivIdentity SecureLogin Single Sign-On Benefits

- Increases the productivity of users and help desk staff by minimizing password resets and downtime associated with forgotten static passwords
- Improves compliance with government regulations and industry mandates related to authentication, audits, and policy enforcement
- Protects resources by enforcing user access rights and reducing the risk of unauthorized access
- Simplifies deployment of strong authentication across networks and applications

ActivIdentity SecureLogin™ Single Sign-On minimizes repetitive password entry and reduces IT help desk costs by providing a secure, automated method to access multiple applications via a single login credential.

The ActivIdentity solution improves security by allowing organizations to automatically generate complex passwords that are less susceptible to theft, guessing, and brute-force dictionary attacks than user-generated static passwords. This capability allows organizations to enforce strong security policies for individual applications while enabling simple and transparent user access. Instead of having to establish, remember, and use a new risk-appropriate password for every application they want to access, users only need to log in when their system starts. This approach simplifies not only user access, but also user credential life cycle management. In addition, it minimizes password resets and other help desk tasks associated with lost or forgotten passwords.

When deployed with ActivIdentity Authentication Client™, ActivIdentity SecureLogin Single Sign-On further reduces help desk costs by enabling self-service emergency access and password resets for users who forget their password or leave a smart card at home.

ActivIdentity ActivClient™ adds strong authentication capabilities to ActivIdentity SecureLogin Single Sign-On by enforcing the use of a smart card or USB token to log in to workstations and to encrypt all user passwords.

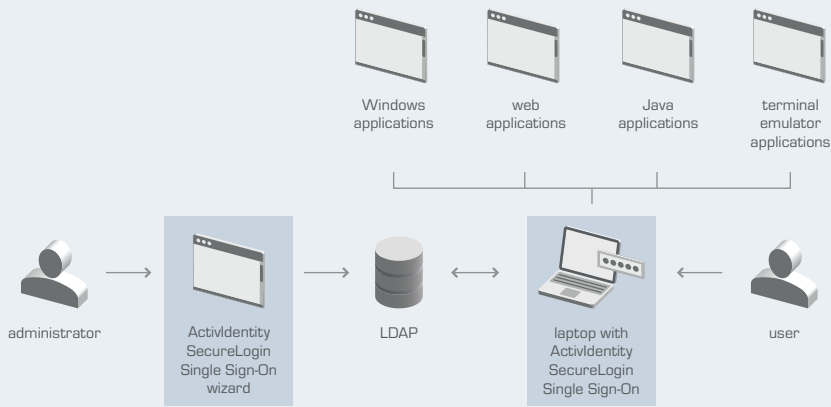


### ActivIdentity SecureLogin Single Sign-On

ActivIdentity SecureLogin Single Sign-On provides single sign-on services to a wide range of enterprise, web-based, Java™, and messaging applications; virtual private network (VPN) clients; terminal emulators; Microsoft® Windows® remote sessions; and more. ActivIdentity SecureLogin Single Sign-On streamlines identity and password management by centralizing passwords and policies in the directory and providing interoperability with leading user provisioning systems. IT managers can provide users with the same credential for remote, offline, and on-premise access to the organization's network.

ActivIdentity SecureLogin Single Sign-On includes the following features and capabilities:

- Powerful support for framed webpages and forms, simplifying single sign-on support for complex websites
- Easy single sign-on enablement with Windows, Java, and web wizards to accelerate the definition process without scripting
- Comprehensive terminal emulator support including UNIX®, ANSI, mainframe, and custom emulators
- Certified Federal Information Processing Standards (FIPS) 140-2 cryptographic libraries for the encryption of user data
- Easy distribution and administration using standard tools and consoles
- Extensive terminal emulator support with more than 30 pre-built definitions
- Self-service alternate authentication method and password resets using the ActivIdentity Authentication Client
- Re-authentication API enables additional security for sensitive applications and data including support for network passwords, smart cards and other authentication methods such as biometrics



### ActivIdentity ActivClient

ActivIdentity ActivClient allows organizations to protect Windows workstations and corporate networks from unauthorized access. By leveraging ActivIdentity ActivClient in combination with ActivIdentity SecureLogin Single Sign-On, organizations can use highly secure smart card-based keys to encrypt user credentials. If desired, IT managers can enforce the presence of the smart card for login operations and require a repeat authentication for access to specific applications.

### ActivIdentity Authentication Client

ActivIdentity Authentication Client provides organizations with an alternate method to access Windows workstations. If users lose a smart card or forget a password, ActivIdentity Authentication Client uses knowledge-based (question and answer) authentication to enable emergency access to ActivIdentity SecureLogin Single Sign-On. Once users access the desktop, ActivIdentity Authentication Client allows them to reset their password. ActivIdentity Authentication Client also enables organizations to support PIN-protected smart card-based static password authentication for Windows login. This extends the advantages of strong authentication with smart cards to organizations that do not issue digital certificates.

## Technical Specifications

|   | ActivIdentity SecureLogin Single Sign-On 6.2  | ActivIdentity Authentication Client 2.0.1 (Emergency Access Edition)  |
|---|---|---|
| <b>System Requirements</b>                                      | <p><b>Client and Management Operating Systems</b></p> <ul style="list-style-type: none"><li>- Microsoft Windows 2000 Workstation, Windows XP, Windows Vista (32- and 64-bit), Windows 7 (32- and 64-bit), Windows Server 2000, Windows Server 2003 (32- and 64-bit), Windows Server 2008 (32- and 64-bit)</li></ul> <p><b>Directories</b></p> <ul style="list-style-type: none"><li>- Microsoft Windows 2000, 2003 and 2008 Active Directory, Microsoft ADAM, Microsoft Active Directory Lightweight Directory Services, Lightweight Directory Access Protocol version 3 (LDAP v3) compliant directories such as Sun Java Systems Directory</li></ul> <p><b>Web Browsers</b></p> <ul style="list-style-type: none"><li>- Microsoft Internet Explorer 6.0, 7.0 or 8.0, Mozilla Firefox 2.0, 3.0 or 3.5</li></ul>   | <p><b>Operating Systems</b></p> <ul style="list-style-type: none"><li>- Microsoft Windows XP Professional, Windows Vista, Windows Server 2003 (x86)</li></ul>                             |
| <b>Compatibility with Select Third-party Software</b>           | <p><b>Remote Sessions</b></p> <ul style="list-style-type: none"><li>- Citrix® XenApp 4.0 and 5.0 (32- and 64-bit), with Program Neighborhood Classic Client and Agent</li><li>- Microsoft Terminal Server</li></ul> <p><b>Terminal Emulators</b></p> <ul style="list-style-type: none"><li>- More than 30 mainframe, UNIX, ANSI, and custom terminal emulators</li></ul> <p><b>Smart Card Middleware</b></p> <ul style="list-style-type: none"><li>- Any smart card middleware with a Microsoft CAPI 2.0 compliant CSP (PKCS#11 interface optional)</li></ul> <p><b>Enterprise Applications</b></p> <ul style="list-style-type: none"><li>- SAP® R / 3®</li><li>- Microsoft Outlook</li><li>- Lotus Notes®</li><li>- Cisco® VPN client</li><li>- Check Point® Firewall-1</li><li>- Windows Live Messenger</li></ul> <p><b>Web Applications</b></p> <ul style="list-style-type: none"><li>- Oracle Forms</li><li>- Standard and framed web pages</li><li>- Complex forms and login pages</li><li>- Java AWT and SWING GUI applets and applications</li></ul> |   |
| <b>Deployment and Management Tools</b>                          | <ul style="list-style-type: none"><li>- Microsoft Management Console Snap-ins, ActivIdentity SecureLogin Single Sign-On Administration Management Utility, ActivIdentity SecureLogin Single Sign-On Personal Management Utility, Microsoft SMS, support for Microsoft Group Policy Object</li></ul>   |   |
| <b>Security</b>   | <ul style="list-style-type: none"><li>- FIPS 140-2 compliant cryptographic libraries</li><li>- Non-repudiation option for administrator access</li><li>- Optional password randomization</li><li>- Optional user data store encryption using smart card (PKI credentials or symmetric key)</li><li>- Application re-authentication using password, smart card, or compliant third-party method (e.g. biometrics)</li></ul>  | <ul style="list-style-type: none"><li>- Emergency Access to Windows using question and answer</li><li>- Windows self-service password reset – available both online and offline</li></ul> |
| <b>Compatibility with Other ActivIdentity Software Products</b> | <ul style="list-style-type: none"><li>- ActivIdentity ActivClient, ActivIdentity Authentication Client, ActivIdentity ActivID Card Management System, ActivIdentity 4TRESS AAA Server for Remote Access</li></ul>   |   |

### About ActivIdentity

**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

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.