



# Single Sign-On Solution

Actividentity SecureLogin

▶ solution brief

## Reduce password pain with SecureLogin

Actividentity SecureLogin provides enterprises with fast and easy access to corporate resources, using a single, secure login. Authenticated users can quickly access their applications with automated login and credential management. It eliminates the burden of remembering multiple credentials for different applications and frees the user from multiple, inconsistent password rules. IT organizations build efficiencies by streamlining and applying consistent and secure credential management policy, cutting down the number of passwords issued to users, and reducing time spent on administration, support and training.

### Benefits to enterprises

#### Reduce help desk support costs

According to leading analysts single sign-on can reduce help desk support costs by up to 40%. Users no longer need to remember as many credential sets with single sign-on, meaning fewer calls to reset passwords or unlock accounts.

#### Increase user convenience

SecureLogin simplifies access to multiple systems and applications, increasing convenience to users. SecureLogin offers optional password storage on smart card capability.

#### Increase user productivity

Reduce the time users spend managing credentials, logging into applications and waiting for credential resets.

#### Reduce exposure to risk

Mitigate exposure to risk from recorded credentials, reused credentials, shared credentials, or easily guessed static passwords.

#### End user managed single sign-on capability

Central administrative control allows administrators to determine how much single sign-on application functionality the end user can see/use (client can be fully user-managed).

#### Assist with regulatory compliance

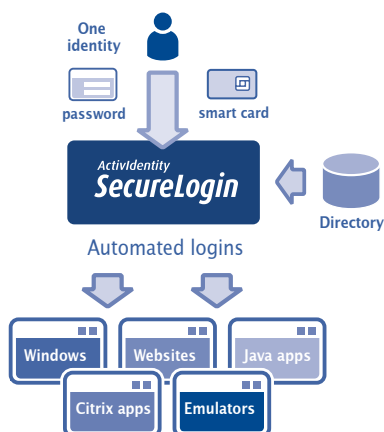
Comply with mandates and government regulation for identity, privacy, policy enforcement, audit and authentication services.

### Faster deployment

By addressing credential management challenges, SecureLogin helps organizations strategically prepare for their future application deployments. Implementing SecureLogin helps organizations roll out new applications without creating additional passwords for users to manage, thus speeding deployment and reducing training efforts.

### How it works

SecureLogin is a single sign-on solution that supervises users access to information by storing, retrieving, and maintaining enabled application credentials. SecureLogin has no server back-end architecture. Client software is installed at every workstation. Once SecureLogin confirms a user's identity, it launches, retrieves and submits the user's credentials from the credential store in the directory into the application login when prompted. User data is stored on the directory in each user object and can be synchronized on a users smart card.



### Highlights

SecureLogin is a complete single sign-on solution designed to automate credential management and simplify access.

#### Fast access to any application

SecureLogin includes out-of-the-box support for a large range of enterprise applications and environments, including Microsoft®, Novell®, Citrix®, Entrust®, Lotus®, SAP® as well as in-house developed applications.

#### Automated credential management

Applications may have various credential management policies, intervals for changing credentials, and different length or character set requirements. SecureLogin automatically handles the processing of such requests to increase security without affecting the user.

#### Non-intrusive integration

Actividentity's approach to single sign-on supports new applications with easy-to-use wizards which make supporting in-house applications simple. It has native support for in-house and out-of-the-box applications.

#### Advanced Security Methods

SecureLogin is the perfect combination with smart card based network authentication. SecureLogin can be used with other Actividentity products to add additional levels of security into your environment—at the most important places. These additional levels of security include support for smart cards, PKI, and one-time passwords (OTP).

# ▶ ActivIdentity Single Sign-On Solution

## An essential component of identity management

Identity management platforms provide a range of identity-based services such as web access, user management, and provisioning. SecureLogin extends the value of an identity management deployment to deliver benefits directly to the end user, providing identity driven single sign-on access to all enterprise applications.

### Advantages for provisioning deployments

Provisioning systems automate account management and centralize allocation of resources to users, however users must still contend with entering and managing credentials after the accounts have been created.

SecureLogin strengthens the security and end user convenience of a provisioning deployment by managing authentication for the user. Using a provisioning connector, provisioning systems can securely deliver application credentials to the SecureLogin credential store. The end user has immediate single sign-on access to applications from the very first login.

### Advantages for web access management deployments

Web access management software leverages directory server-based sources of identity information and user management tools to help organizations administer identity and security controls over their user population.

SecureLogin complements web access

management with managed enterprise authentication services. Organizations can take advantage of single sign-on access to client/server, desktop, terminal, as well as web-based applications—while using the web access controls, user management, and directory server from their web access management deployment. These options provide even greater flexibility to meet specific security requirements, achieve greater credential management cost reductions, and maximize the value of existing identity investments.

### Consolidation of credentials on a smart card device

SecureLogin can store single sign-on credentials in a PIN protected generic container on a smart card.



## Fits your business processes

Getting results from good security practices depend on getting the proper fit with the way that a company does business. SecureLogin offers a number of features designed to optimize deployment in any environment.

Every business has their own requirements

for identifying their users. Using different authentication methods (or multiple methods combined together) helps businesses select the method that best meets their specific needs for identity, security, and convenience.

With SecureLogin organizations can start their deployment by reusing existing passwords (such as the Windows login from Active Directory) and upgrading to multi-factor authentication support as their requirements evolve.

SecureLogin has the option to store password credentials onto a smart card

for greater security and accessibility.

ActivIdentity SecureLogin uses existing sources of identity such as corporate LDAP directories, Active Directory, or identity management repositories. Using existing identity data reduces administrative effort and maximizes the value of existing directory investments.

SecureLogin can encrypt the user directory data store utilizing the PKI based credentials from a smart card. SecureLogin also provides a separate standalone utility to allow smart card based static password workstation login (non PKI).

## Compelling Return on Investment (ROI)

SecureLogin offers a compelling return on investment and a significant reduction on support costs. Help desk costs are minimized by reducing the number of credentials that users need to remember.

Cut down on lost or forgotten credential support calls to reduce help desk load by up to 40% (according to leading analysts).

Instead of waiting to enter or remember usernames and passwords, credentials are

automatically entered, resulting in cumulative time savings.

You also receive beneficial returns by avoiding credential related pit-falls. Minimizing exposure to risk helps avoid unauthorized access and protects your corporate image.

Eliminating credential frustration can increase employee satisfaction and improve the user's perception of the work environment.

In order to examine the potential cost savings and ROI, please visit our website or contact us for more information.

[www.actividentity.com](http://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	<a href="mailto:info@actividentity.com">info@actividentity.com</a>

**ActivIdentity™**