

# Actividentity SecureLogin® Kiosk

➤ Fast user switching for shared workstations

## Rapid access to computing resources

Many industries such as healthcare and manufacturing use shared workstations to provide employees with rapid access to computing resources. Compliance (HIPAA, Sarbanes-Oxley, GLBA, Basel II) and security requirements have led to complex password requirements on these workstations. As a result, shared workstation usage is difficult due to the number and complexity of passwords. Frustrated staff tend to bypass security by sharing passwords or leaving applications open for the next person to use.

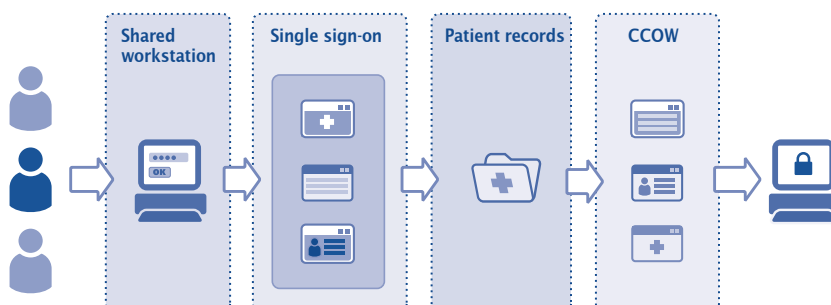
SecureLogin® Kiosk makes shared workstations easy to use, secure and keeps users accountable for their online activity. SecureLogin Kiosk works together with SecureLogin SSO for fast user switching in a shared workstation environment: users log on once (via password, smart card, USB token, active proximity badge, biometrics, or a combination of these), and have automatic access to applications without further password prompts.

## Key features

### Fast login, fast logoff

- Users log on once, with no more password prompts from applications.
- SecureLogin Kiosk gracefully closes applications to save data in case users need to leave quickly.

## SecureLogin Kiosk architecture overview



Kiosk provides fast access to medical applications on shared workstations.

- Applications with long startup times can stay running and switch users without having to launch and close every session.

### Supports leading applications

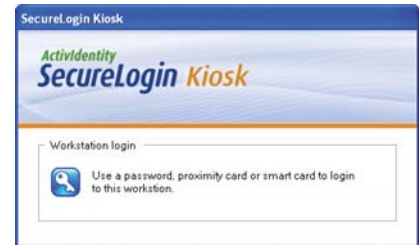
- Works with nearly all desktop, terminal and web-based applications.
- Supports medical applications such as Cerner Millennium® and MEDITECH applications.
- Supports SSO to and within Windows® Terminal Services and Citrix® sessions.
- Integrated support for active proximity badges such as the Ensure Technologies™ Xyloc™.

### Flexible Deployment

- Configurable automatic logoff time out set which applications stay open or which ones are closed when users log off.
- Specify applications to save data before log off.

### Complements identity management projects

- Supports identity management provisioning systems from Microsoft®, Novell®, Sun®, and IBM®.
- Supports Fusion from Carefx™ for patient information aggregation.
- Provides context management in CCOW-enabled applications for simplified access to patient data.
- Removes complexity from navigating menus and searching for records in every application used during the work session.



## Benefits

### Improves user satisfaction

Users often perceive password prompts as an impediment to getting work done. SecureLogin Kiosk makes computer access easy, fast, and secure.

### Addresses regulatory compliance and accountability

Behind the scenes, applications stay safe through randomized strong passwords that users don't need to memorize.

### Rapid identification

When combined with active proximity badge authentication, SecureLogin Kiosk automatically recognizes users when they are near. Users do not have to type in their username to get started.

### Prevents unauthorized access

Workstations in high traffic areas stay locked when not in use. With an active proximity badge, SecureLogin Kiosk automatically locks the workstation when the user walks away. With a smart card or USB token, the workstation is locked automatically when the device is removed.

### Kiosk components

- SecureLogin Kiosk
- SecureLogin Kiosk Admin Pack Server

### System requirements

- Microsoft Windows-based PC with 64MB memory, 150 MB free disk space
- Microsoft Active Directory
- SecureLogin SSO

### Optional components

SecureLogin Kiosk can be configured with:

- ActivClient (for smart card support)
- Ensure Technologies™ ETSecure Service for deployment with Xyloc™ proximity recognition systems.

### Thin Client

- Citrix® Presentation Server™
- Microsoft® Windows Terminal Services

### Proximity device

- Ensure Technologies™ XyLoc™

### Authentication methods

- Windows password login through Active Directory®
- Smart Card, USB tokens and biometrics with ActivClient™
- Proximity-based authentication with Ensure Xyloc + Microsoft Active Directory password

### Directory

- Microsoft Active Directory

### Operating systems

- Client: Microsoft Windows 2000, Windows XP Professional
- Server: Microsoft Windows 200 Server, Windows Server 2003

### Security

- Data encryption through Microsoft Crypto API
- Communications secured via SSL

### Management tools

- Microsoft Management Console
- Microsoft Group Policy Management Console (GPMC)
- Microsoft Administrative Tools

### Smart card compatibility

- Smart Cards & USB Tokens from ActivIdentity, Atmel®, Gemalto®, Giesecke & Devrient, Oberthur
- Support for the U.S. DoD Common Access Card
- Support for FIPS 201 certified Personal Identity Verification (PIV) cards

### Biometric compatibility

- Authentec including Verifi P4000 and P3400 readers
- BIO-key various readers
- Digital Persona including URU 4S-U1 readers
- Precise including 100 XS, 100 MC, AX100 XS readers
- Sagem including MSO100, 300, 1300 readers
- SecuGen including FDU01 and FDU02 Upek various readers

### Identity management and user provisioning

- CAT™ eTrust Admin
- IBM® Tivoli® Identity Manager
- Novell® Identity Manager
- Sun Java™ System Identity Manager

### Related data sheets

- SecureLogin SSO
- ActivClient

### Partners



To find out more about ActivIdentity products, visit our website

[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>

