



# The BOX



**that is changing  
Single Sign-On for Healthcare**



Password security and user access issues are major issues for healthcare organizations. Add to this regulatory compliance—Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley, and others—and the problem is even more demanding. While single sign-on (SSO) technology is not new, existing solutions have been expensive, time consuming and rarely lived up to expectations. Until now.

Imprivata® OneSign™ Single Sign-On has changed all that. OneSign helps healthcare organizations benefit from increased user productivity and reduced password management costs by enabling SSO to all your enterprise and sensitive clinical applications.

OneSign is so radically easy, simply smart and uniquely affordable, it delivers on one very important promise almost immediately: rapid return on your investment. **Read on, and you'll find out how.**



# OneSign: Single Sign-On for Healthcare

## ➔ Radically easy

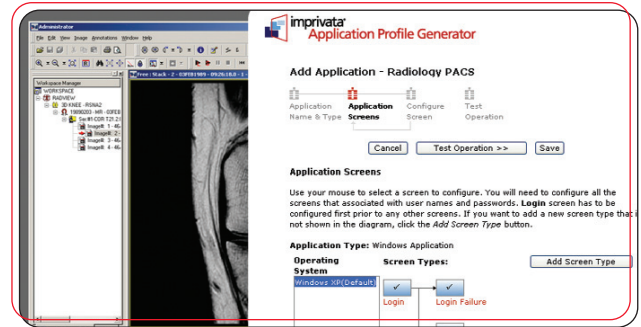
### *Convenient*

From the beginning, OneSign Single Sign-On was designed to make password management easy for IT and end users alike. Implementing and managing it is extremely fast and simple.

- OneSign meets the needs of the mobile healthcare professional—and eliminates caregiver distraction. Users simply log on to applications as always, and need no training or modifications to their desktop environment.
- OneSign recognizes when new appliance versions, SSO profiles, or user security policies are added or changed and automatically handles all updates.
- Organizations can enable Roaming Sessions and Personalized Drive-Mapping by extending OneSign events to launch an

unlimited set of critical business functions.

- OneSign's administrator console provides an intuitive, easy to navigate, Web-based interface, making enterprise single sign-on easy to install, configure and deploy. In a matter of days, you can fully SSO-enable your organization.



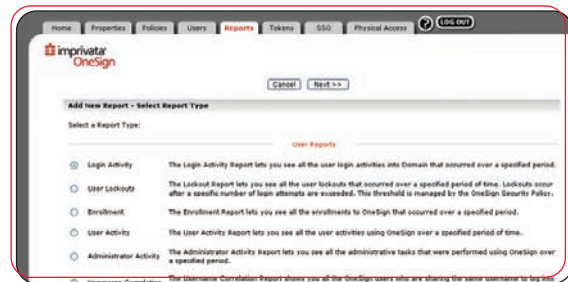
## ➔ Simply smart

### *Compliant and Secure*

With regulatory guidelines mandating stricter HIPAA compliance, you benefit from OneSign's hardened enterprise SSO appliance. OneSign Single Sign-On is designed to be smart enough to do much of the work for you, anticipating and automating redundant tasks.

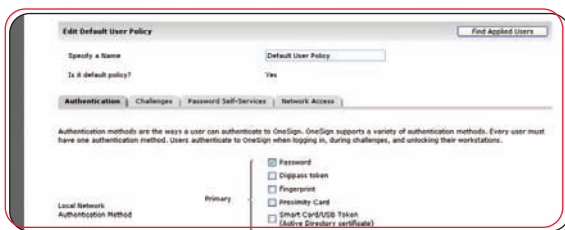
- OneSign automates password policy implementation—creating unique, strong passwords behind the scenes to ensure compliance and patient data privacy. It performs password changes automatically on behalf of your users, ensuring stricter security and eliminating security breaches associated with passwords written on sticky notes affixed to keyboards and monitors.
- With built-in support for a broad range of authentication methods such as passwords, finger biometrics, ID tokens, proximity cards, and

- Built-in monitoring provides detailed audit logs of which users accessed which applications and when, including all password change activity. Detailed access logs and reports



give you the ability to refine and strengthen security policies and enforce HIPAA compliance across all applications.

- OneSign's intelligent Application Profile Generator™ (APG) technology SSO-enables all clinical and enterprise apps—legacy, client/server, or Web-based—out of the box. There is no custom scripting, no connectors to build, and no long and expensive custom integration projects to manage.
- OneSign's reliability enhances patient data safety. The appliance is shipped in a redundant pair configuration, providing seamless failover. System back-ups can be automatically run, transferred for storage each day, then restored from a back-up file in minutes for disaster recovery.



smart cards, OneSign offers a smart and effective way to increase security while leveraging the benefits and convenience of SSO.

## ➔ Uniquely affordable

### *Lowest TCO Anywhere*

OneSign's fast installation and deployment time and low ongoing maintenance costs deliver instant help desk cost reduction—and with that, immediate financial return.

- As a self-contained appliance, OneSign delivers all the functionality needed to effectively implement and manage

single sign-on. There is nothing else to buy—no custom scripting or costly integration.

- Changes to policy, applications or user profiles can be administered and transparently applied in a matter of minutes from the administrator's console, without impacting user productivity.
- Companies see lower costs and increased staff productivity due to greatly reduced help desk and password reset calls.

# What's inside **The BOX**

## ■ **Application Profile Generator: Radically Easy**

The OneSign Application Profile Generator (APG) enables SSO and password change for ALL enterprise applications—without writing logon scripts, building custom connectors or modifying applications. APG's drag-and-drop paradigm automatically learns login and password change behavior for even the most challenging applications.

## ■ **Support for Shared Workstation Environments**

OneSign addresses the unique needs of the highly mobile healthcare professional, including:

- **Fast user switching** – OneSign lets multiple users securely share workstations without having to log out of the desktop. The desktop state of each user can be maintained for all Citrix and Terminal Server hosted applications.
- **Roaming users** – As clinicians roam from one shared workstation to another, OneSign seamlessly manages connects and disconnects to their Citrix or Terminal Server hosted desktop, ensuring a smooth roaming experience.
- **Compliance**—OneSign tracks the access events of each user on the shared workstation and provides one-button and inactivity screen locking.

## ■ **Authentication Management for Fast & Secure Access**

OneSign supports all major forms of authentication without requiring custom integration with device vendors. Authentication methods include strong password, the industry's only finger biometric identification technology, passive and active proximity cards such as Xyloc, smart cards, and one-time-password tokens for local or remote access.

## ■ **Comprehensive User & Computer Policy**

Policies can be assigned to specific computers, overriding policies defined at the user level. For example, OneSign can be configured so that a doctor has a five minute inactivity lock when logged onto his office computer but has a seven hour inactivity lock when logged onto an operating room workstation.

## ■ **Automate Application Password Changes**

Administrators can implement password policy across all SSO-enabled applications based on the user's primary authentication. OneSign can cycle complex application passwords behind the scenes on the user's behalf, making application access more secure while freeing clinicians from change password headaches.

## ■ **Integration with Best-of-Breed Context Management**

OneSign integrates with Fusion from Carefx™ to create a user-driven, patient-centered clinical workspace that synchronizes context across multiple applications, increasing user productivity and patient safety. Upon launching the initial application and selecting a patient, encounter or observation, Fusion from Carefx™ automatically finds and links related patient information across all other applications.

## ■ **Integration with Best-of-Breed User Provisioning**

Third party provisioning systems can provision and de-provision application accounts within OneSign, increasing “Day One” user productivity and ensuring that application credentials in OneSign are always up-to-date. Best-of-breed provisioning partners with OneSign connectors include Courion® and Fischer International™.

**OneSign –  
The Enterprise  
SSO Solution  
of Choice  
for Healthcare**

**“A key advantage of OneSign is its ability to take the complexity and risk out of password management and maintenance.”**

—Charles Christian  
Director of IS  
Good Samaritan Hospital

**“OneSign has been a huge success. From an IT perspective, this has been the most successful product I've ever dealt with in terms of user satisfaction.”**

—Stefan Hopper, CIO and Director of IS, Gateway Health System

**“As an appliance-based solution, OneSign is non-intrusive and installs easily. Because OneSign required no changes to our existing applications, we were able to have it up and running within 30 days.”**

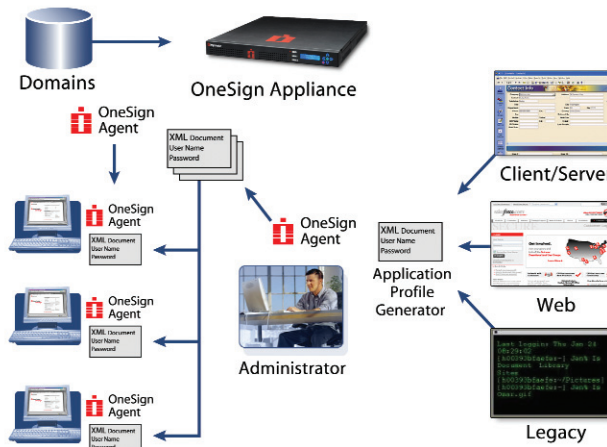
—Burt Ridge, CIO, Laughlin Memorial Hospital



**Rated by KLAS as the best  
single sign-on solution of 2006.**

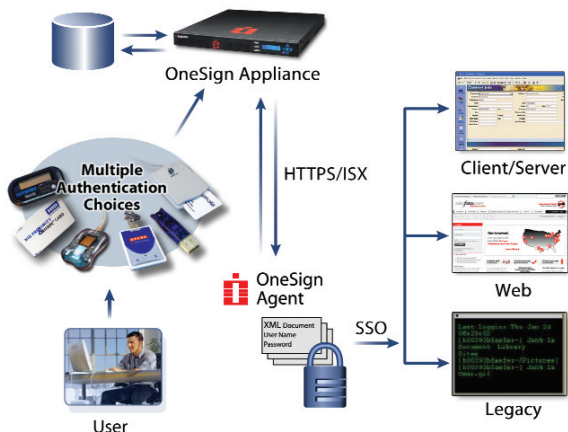
**OneSign: Single Sign-On for Healthcare**

## ➔ OneSign Administration Enablement



Using the OneSign browser-based interface, the administrator starts the enrollment and deployment process by synchronizing OneSign with existing domains and user directories. The OneSign APG then learns the password behaviors of all applications and uses that information to create an XML profile for each application. The profiles, together with their corresponding policies, are then stored centrally on the OneSign Appliance. The OneSign Agent on each user's PC receives the latest set of profiles, policies and credentials distributed every time a user is authenticated.

## ➔ The OneSign User Experience



OneSign handles primary authentication through a pass-through extension of the Windows logon. The OneSign Agent then establishes a secure https:// session with the Appliance using double-blind encryption and disposable session keys. The OneSign Agent observes the application screens as defined in their profiles and behaves as needed to enable SSO and password management according to the latest policy for each individual user.

**Imprivata OneSign Single Sign-On provides a radically easy, simply smart and uniquely affordable enterprise single sign-on solution that delivers rapid ROI, increased productivity and regulatory compliance. In other words, it's the box that's changing ESSO.**

**To learn more, visit [www.imprivata.com](http://www.imprivata.com) or call 877-OneSign (877-663-7446).**



**Corporate Headquarters**  
 10 Maguire Road  
 Lexington, MA 02421  
 v 781 674 2700  
 f 781 674 2760

## TECHNICAL SPECIFICATIONS

### Application Environments Supported

- ALL browser-based applications running in Internet Explorer 5.5 SP2 or higher on supported Windows OS.
- ALL Mainframe, AS/400, UNIX, other legacy applications accessed via Terminal Emulators (TEs)
  - TEs that support a HLLAPI interface on supported Windows OS
  - Non-HLLAPI TEs
  - Web-to-Host clients
  - Console-based applications launched from a Windows command line
- ALL Win32 client-server or client applications on supported Windows OS
  - Windows applications
  - Java applications using SUN, Oracle, or IBM JVM
  - Custom and legacy applications running on a supported Windows OS
- ALL Clinical applications for Healthcare

### Context Management

- Interoperability with Carefx provides end-users with single sign-on (SSO) to network resources and to both CCOW and non-CCOW applications.

### Administration Console Requirements

- Internet Explorer 6.0 SP1 or later running on Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003. USB is required for finger biometrics and proximity cards.

### Client Systems Supported

- Internet Explorer 5.5 SP2 or later running on Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003. USB is required for finger biometrics and proximity cards.

### Directories Supported

- Microsoft Active Directory 2000 / 2003 Server, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID) 10g, Novell Netware 5.1 running NDS 8.0 or later, Novell eDirectory 8.0 (8.1 required for SSPW Management), IBM Tivoli LDAP.

### Appliance

- Pair of ready-to-use redundant 1U rack mountable servers. Failover is included. Operating system is SUSE® LINUX Enterprise 9 from Novell.

### Internationalization

- Unicode multi-byte character support on the Agent and appliance for capturing and proxying Usernames and Passwords in multi-byte character sets. Interface remains in English with the exception of localization enablement. Agent dialogs also in French and German.