

The BOX



that is changing Enterprise Single Sign-On

Password security and user access issues are becoming major issues for organizations. Add to this regulatory compliance — Health Insurance Portability and Accountability Act (HIPAA), GLBA, Sarbanes-Oxley and Basel II — 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 has changed all that. Using breakthrough technology, OneSign helps organizations benefit from increased user productivity and reduced password management costs by enabling SSO to all your enterprise applications.

Truth is, the technology behind 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

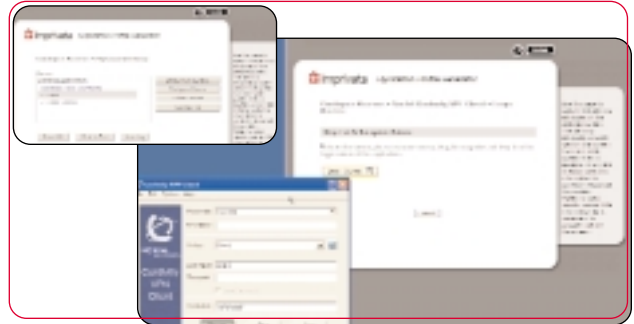
The solution for password management

➔ Radically easy

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

- Our intelligent Application Profile Generator (APG™) technology does all the work. There is no custom scripting required, no connectors to build and no extensive or expensive custom integration projects to manage. With OneSign, companies can enable SSO for all enterprise applications — legacy, client/server or Web-based — out of the box.
- OneSign's administrator console provides an intuitive, easy to navigate, Web-based interface. Making enterprise single sign-on (ESSO) easy to install, configure and deploy. In a matter of days, you can fully SSO-enable your organization.

- The OneSign Agent™ automatically handles updating for you by recognizing when new versions, application SSO profiles or user security policies are added or changed.
- It's easy for users, too. They log on to their applications as always, and require no training or modifications to their desktop environment.



➔ Simply smart

A hardened enterprise SSO appliance built on patent-pending technology, OneSign was designed to be smart enough to do much of the work for you because we anticipated and automated the redundant tasks.

- OneSign automates password policy implementation — creating unique, strong passwords behind the scenes to ensure compliance. It performs password change activities automatically on behalf of the users, ensuring a higher degree of security. It eliminates security breaches associated with sticky notes. And, OneSign decreases costly help desk calls associated with password resets.

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

- Built-in monitoring provides an accounting of which users accessed which applications and when, including all password change activity. Detailed access logs and reports give organizations the ability to refine and strengthen security policies and enforce regulatory compliance across all applications.



- With built-in support for various authentication methods such as passwords, ID tokens, proximity cards, smart cards

- The OneSign Appliance is shipped in a redundant pair configuration, providing seamless failover. System back-up can be automatically run and transferred for storage each day without administrator effort. The system can be restored from a back-up file in minutes for disaster recovery.

➔ Uniquely affordable

OneSign's low total cost of ownership, short implementation time and quick user adoption delivers instant help desk cost reduction — and with that, immediate financial return.

- As a self-contained enterprise SSO 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. Users remain productive, and ongoing day-to-day management is minimal.
- Companies see decreased costs and increased staff productivity due to greatly reduced help desk and password reset calls.

OneSign is the enterprise single sign-on solution that delivers on its promise: making password management and security truly manageable.

What's inside the box

■ Application Profile Generator

The OneSign Application Profile Generator (APG) enables SSO and password change support for ALL enterprise applications — without writing logon scripts, building custom connectors or modifying existing code. APG's point-and-click paradigm automatically learns logon and password change behaviors for even the most challenging applications — including native Java clients, Telnet emulators, Web-to-host applications, frame-based Web applications and many more.

■ Self Service Password Management

With this module, users can easily reset or be notified of their own network and application passwords without help desk intervention. Administrators can set identity verification thresholds for users, or groups of users who are simply prompted to answer a set of random questions, and, once authenticated, OneSign delivers the service. This service can be accessed either by users on the network or via the Web.

■ Monitoring and Reporting

The OneSign Agent allows organizations to monitor, capture and log password-related user access events in a centralized database. Easy-to-use detailed reporting can strengthen security and enforce regulatory compliance across all applications. Now, for the first time, administrators can easily monitor access records for every user, application or workstation in one, central location — even revealing users that may be sharing credentials to confidential applications.

■ Automated Application Password Changes

Now with OneSign, administrators can implement a clear, straightforward password policy across all SSO-enabled applications based on users' primary authentication. For additional security measures, OneSign is able to cycle complex application passwords behind the scenes on the users' behalf. This allows organizations that require certain application passwords to be changed periodically to handle the changes automatically.

■ Intelligent Agent

The intelligent OneSign Agent is designed to dynamically self-update whenever new SSO-enabled applications or security policies are updated on the appliance. This feature

simplifies deployments without adding administrative overhead. Since the session is tied to the user identity, not the desktop, SSO credentials can be securely delivered to an authenticated user anywhere in the enterprise, making single sign-on possible whether users are on- or off-line.

The shared workstation SSO Agent supports multiple separate, secure user sessions in a shared workstation environment. With a one button lock/unlock hot key, users can single sign-off all running applications when a new user presents a logon request.

■ A Scalable and Extensible Web Services Architecture

OneSign uses a standard Web services architecture for providing secure communications between distributed OneSign Agents and the OneSign Server. OneSign business logic running within the application server provides centralized services accessible to only OneSign Agents for user authentication, biometric identification and SSO session management. The OneSign architecture leverages not only the speed, security and reliability of Web Services for critical Agent-to-Server communications, but also its ability to offer a rich browser experience for OneSign administration. Open standards within the Server design offers an extensible and scalable solution suitable for rapid integration with other identity management solutions such as Web SSO, Auditing and Provisioning.



The OneSign reviews are in:

Excellent 

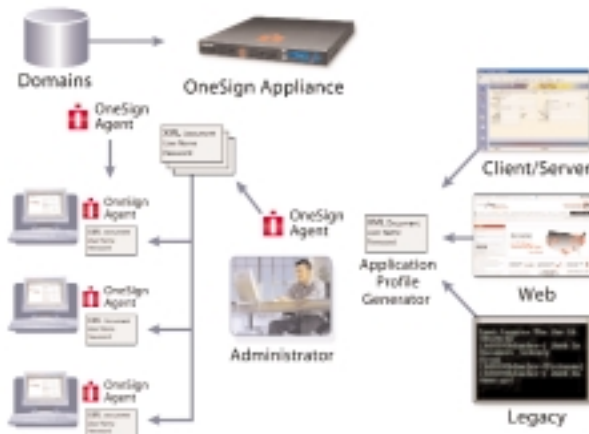
Five out of five stars



OneSign truly allows
easy implementation
and deployment

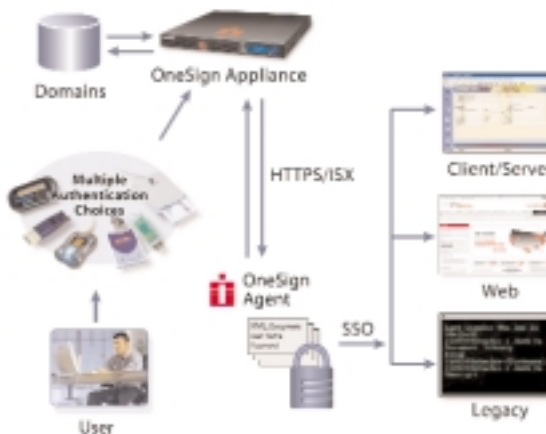


➔ OneSign Enrollment and Deployment



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 one. The profiles, together with their corresponding policies, are then uploaded and 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 an Imprivata Secure Exchange 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 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 or call 877-OneSign (877-663-7446).



Corporate Headquarters
10 Maguire Road, Building 2
Lexington, MA 02421
v 781 674 2700
f 781 674 2760

Imprivata EMEA
Forsyth House, 77 Clarendon Rd.
Watford, Herts WD17 1LE
United Kingdom
v +44 (0)1923-813511
f +44 (0)1923-813501

TECHNICAL SPECIFICATIONS

Administration Console Requirements

Internet Explorer 6.0 or greater running on Windows NT 4.0 SP5, Windows 98 Second Edition, Windows 2000, or Windows XP Professional. USB is required for finger biometrics.

Client Systems Supported

Internet Explorer 5.5 SP2 or greater running on Windows NT 4.0 SP5, Windows 98 Second Edition, Windows 2000, or Windows XP Professional. USB required for finger biometrics.

Supported User Directories

Microsoft Active Directory 2000 or 2003 Server, NT 4.0 Domain, Sun ONE LDAP Directory Server, Oracle Internet Directory (OID), Novell Netware 6.0 running NDS 8.0 or higher, Novell eDirectory 8.0 (8.1 required for Self-Service Password Management module).

Supported Application Environments

Web (browser-based) applications running in Internet Explorer 5.5 SP2 or higher on supported Windows OS.

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 may be learned using the Imprivata OneSign Application Profile Generator (APG)
- Console-based applications launched from a Windows command line

Win32 client-server or client applications on supported Windows OS

- Windows applications
- Java applications using SUN, Oracle, or IBM JavaVirtual Machines (JVMs)
- Custom and legacy applications running on a supported Windows OS

Context Management for clinical applications — Interoperability with Carefx provides end-users with single sign-on (SSO) not only to network resources and non-CCOW applications but also to applications utilizing CCOW.

Appliance

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

Internationalization

Support for storing and retrieving user names and passwords for all countries in Western Europe. Interface remains in English with the exception of L10N enablement — Agent dialogs in French and German.