

The BOX



that is changing Single Sign-On

Password security and user access are major issues for most organizations. Add to this regulatory compliance—Health Insurance Portability and Accountability Act (HIPAA), Sarbanes-Oxley (SOX), Gramm-Leach-Bliley Act (GLBA), Homeland Security Presidential Directive-12 (HSPD-12), Federal Information Processing Standard (FIPS) 201, 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™ Single Sign-On has changed all that. Using breakthrough technology, OneSign Single Sign-On 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.



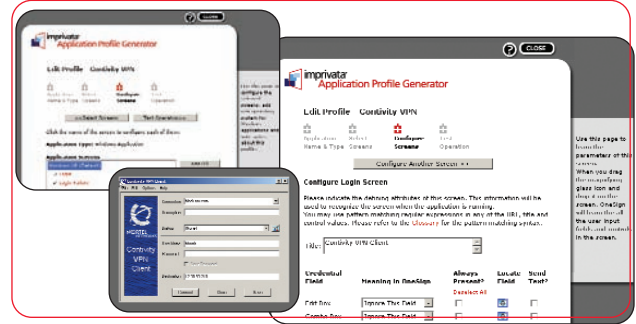
OneSign Single Sign-On: The Solution for Password Management

➔ Radically easy.

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

- Our intelligent Application Profile Generator™ (APG) technology SSO-enables all enterprise applications—legacy, client/server, or web-based—out of the box. There is no custom scripting required, no connectors to build, and no long and expensive custom integration projects to manage.
- OneSign’s administrator console provides an intuitive, easy to navigate, web-based interface, making single sign-on easy to install, configure and deploy. In a matter of days, you can fully SSO-enable your entire 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.

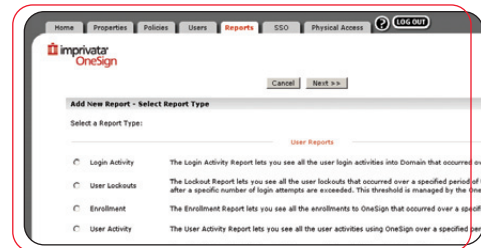


➔ Simply smart.

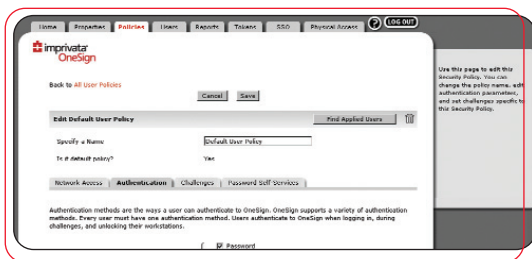
A hardened appliance built on patent-pending technology, OneSign was designed to be smart enough to do much of the work for you because we anticipated and automated the redundant tasks.

- OneSign Single Sign-On automates password policy implementation - creating unique, strong passwords behind the scenes to help support compliance needs. It performs password changes automatically on behalf of the users, ensuring stricter security. It eliminates security breaches associated with passwords written on sticky notes or hidden under keyboards. And, OneSign Single Sign-On decreases costly help desk calls associated with user password resets.
- Organizations can extend OneSign events to launch an unlimited set of critical business functions using OneSign Extension Objects.

- With built-in support for various authentication methods such as passwords, ID tokens, active or passive proximity cards, smart cards 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.
- 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 appliance, OneSign delivers all the functionality needed to effectively implement and manage SSO. 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 on-going day-to-day management is minimal.
- Companies see decreased costs and increased staff productivity due to greatly reduced help desk and password reset calls.

What's inside **The BOX**

■ Automate Application Password Changes

With OneSign Single Sign-On, administrators can implement a clear, straightforward password policy across all SSO-enabled applications based on users' primary authentication. For additional security measures, OneSign Single Sign-On 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.

■ 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 or administrator-created questions. Once authenticated, OneSign Single Sign-On delivers the service. This service can be accessed either by users on the network or via the web.

■ Broad Support for Strong Authentication

The OneSign appliance supports major forms of authentication out of the box—without requiring any custom integration with device vendors. Authentication methods include password, strong password, finger biometric authentication or identification, active and passive proximity cards, smart cards, USB tokens, and Kerberos authentication. Administrators decide which users should have which authentication modes, and whether they should upgrade their authentication options over time.

■ Application Profile Generator (APG): Point-and-Click instead of Expensive Scripting

The 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.

■ Compliance: 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.

■ Provisioning Support

OneSign Single Sign-On provides provisioning support based

on the industry standard Service Provisioning Markup Language (SPML). SPML-based provisioning support allows users - and their network and application credentials - to be automatically provisioned and de-provisioned in OneSign Single Sign-On, eliminating the need to ever issue passwords to your users. New users, applications, and password resets are automatically reflected in OneSign. Imprivata provisioning partners providing out-of-the-box OneSign provisioning connectors include Courion and Fischer International. Check with your OneSign representative for the most up to date list of OneSign provisioning partners and connectors.

■ OneSign Extension Objects: Roaming Desktops, Drive-Mapping, and More!

Organizations can now extend OneSign events to automate or integrate with an unlimited set of critical business functions. This is done through the execution of procedure code that can be associated with any OneSign Agent event. Examples:

- Roaming User Desktops
 - session management across workstations
- Personalized Drive-Mapping
 - desktop follows user switching workstation
- Automated Password Synchronization
 - across multiple workstations
- Event-Based User Messages
 - executing a start-up command upon login

These procedures can consist of DOS command sequences, Javascript, or Visual Basic Scripts. Any pre-defined OneSign Agent event can trigger one or more procedures.

The OneSign reviews are in:



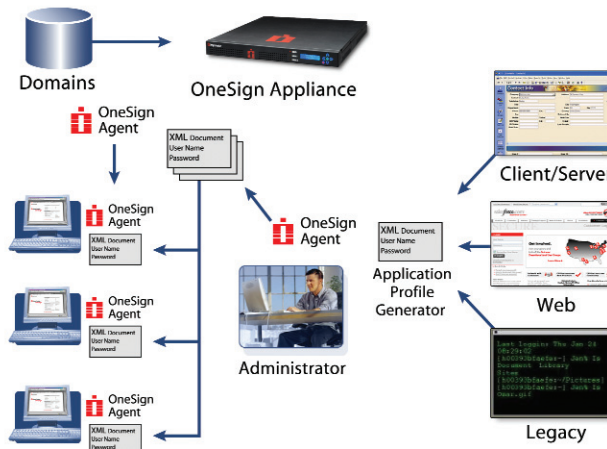
Excellent

Five out of five stars



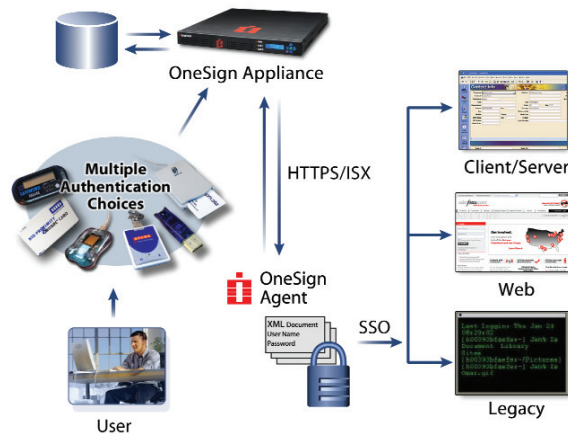
OneSign: The Solution for Password Management

➔ OneSign Enrollment and Deployment



Using the OneSign browser-based interface, the administrator starts the enrollment and deployment process by synchronizing OneSign Single Sign-On 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 solution that delivers rapid ROI, increased productivity and support for regulatory compliance.

In other words, it's the box that's changing SSO.

To learn more, visit 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

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

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.