# **imprivata®**

# **HE HAS EIGHT PASSWORDS, BUT ALL HE HAS MEMORIZED IS THE HELPDESK NUMBER.**

## **HELP FOR THE PASSWORD-CHALLENGED AND STRESSED HELPDESKS**

You know that the most secure application passwords are strong ones—those that contain at least eight characters, upper and lower case letters, random numbers, punctuation marks, and symbols. Their complexity makes them difficult to crack, but strong passwords are also difficult for authorized users to remember—and the more applications a person uses, the more passwords there are required to remember. That's why so many users resort to writing passwords down and sharing them with others, leaving passwords where they can be seen and used by unauthorized people. This can lead to the theft or sabotage of confidential information and the violation of government and industry regulations that mandate the protection and privacy of customer and confidential data.

The complexity of strong passwords can also result in costly inconvenience and frustration for both users and IT departments. Users who forget their passwords are frequently locked out of their systems and unable to do their work. They then call the IT helpdesk to request resets for their forgotten passwords, creating an unnecessary burden on IT resources and substantial costs—all of which can inhibit more important work from being accomplished.

## **IMPRIVATA ONESIGN® SINGLE SIGN-ON SOLVES THE PASSWORD PROBLEM**

With Imprivata OneSign Single Sign-On (SS0), a single action of user authentication permits users to access all desktops and applications they are authorized to use, thereby eliminating the need to remember and enter multiple difficult passwords. Imprivata OneSign Single Sign-On makes it possible to establish and enforce strong password policies without putting an undue burden on users. Without multiple passwords to

manage, users can maintain productive workflows without the inconvenience of calling the IT helpdesk with password reset requests.

Imprivata OneSign Single Sign-On takes the complexity and cost out of password management by providing support for all applications—legacy, Windows, Java, Web, and more. In doing so, Imprivata OneSign enforces secure and compliant employee access to applications while supporting the auditing and reporting requirements of government regulations. Imprivata Onesign does all that without the need for custom scripting, modifications to existing directories, or changes to user workflows.
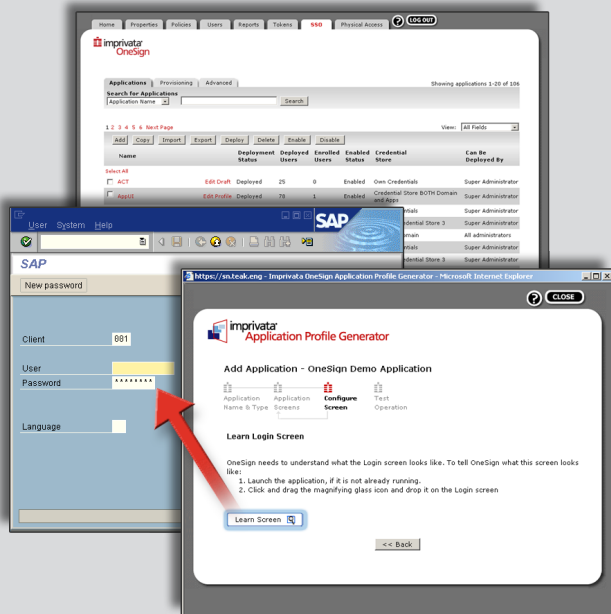
## **BENEFITS OF IMPRIVATA ONESIGN SINGLE SIGN-ON**

- Relieves frustration and enhances user convenience and productivity

- Reduces password administration and helpdesk costs

- Ensures compliance with strong password policies and security regulations

- Provides visibility into all user access activities across disparate applications

# [ WHAT'S INSIDE THE BOX

## RAPID SINGLE SIGN-ON ENABLEMENT FOR ALL APPLICATIONS

Imprivata OneSign's Application Profile Generator® is a patent-pending technology that provides administrators with an easy-to-use, drag-and-drop interface that dynamically profiles all of an application's sign-on behaviors. Imprivata OneSign's single sign-on enablement simplifies the SSO profiling and does not require any scripting, modification of application code, or directory changes.



## BUILT-IN SUPPORT FOR MULTIPLE STRONG AUTHENTICATION OPTIONS

Imprivata OneSign Single Sign-On may be seamlessly coupled with Imprivata OneSign Authentication Management, allowing you to secure the desktop and network by providing native support for a broad range of strong authentication options including fingerprint biometrics, active and passive proximity cards, smart cards, many National Health and ID cards, One-Time-Password and USB tokens.

## SHARED WORKSTATIONS AND FAST USER SWITCHING

Imprivata OneSign offers a variety of workflow solutions for users who share workstations, including fast user switching between multiple, concurrent Windows desktops, as well as secure fast user switching on top of a generic kiosk desktop. Workstation security and data privacy are increased with configurable "hot key" screen locking, inactivity lock/logoff policies, and screen locking by tapping a proximity card/badge.

## SELF-SERVICE PASSWORD RESET

Users can reset their primary domain passwords—securely and conveniently—without making burdensome and costly calls to the IT helpdesk.

## PASSWORD POLICY ENFORCEMENT

For maximum application security, Imprivata OneSign can be configured to enforce password strength during the application expiration/password change process, or handle password changes behind the scenes at regular intervals.

## CITRIX/XENAPP & TERMINAL SERVICES SUPPORT

Imprivata OneSign Single Sign-On supports all XenApp or Terminal Services-hosted applications. Imprivata OneSign can automatically roam the user's remote session when they log into Imprivata OneSign, and automatically lock the desktop of the user's previous workstation when they roam to a different workstation.

> "Imprivata's Single Sign-On solution has tremendously improved our employees' productivity. Without the need to remember an extensive list of passwords, SSO has allowed Verity Credit Union to focus on more important business matters such as the financial needs of our members. Employees quoted that SSO is truly a great addition and quite possibly one of the most useful technical enhancements ever."

> - Jon Wu, *System Engineer II, Verity Credit Union*

## USER PROVISIONING INTERFACE

Imprivata OneSign integrates with user provisioning systems for "Day One" employee productivity. Imprivata OneSign natively interfaces with Courion, Fischer International, and IBM Tivoli, which can provision and de-provision users and application credentials within Imprivata OneSign. That means there's no need to distribute application passwords to users, and everything is managed centrally.

## COMPLIANCE REPORTING

Imprivata OneSign records all computer and application access events in a centralized database, even down to the application screen level. At the push of a button, administrators can run any number of web-based reports, including a report to see which users are sharing passwords, who accessed which applications, when and from where, and all the application accounts that belong to a particular LDAP user.

## THE IMPRIVATA ONESIGN PLATFORM

Imprivata OneSign Single Sign-On is a module within the Imprivata OneSign Platform. Imprivata OneSign is an identity and access management platform that integrates user authentication, user access, password management and aggregated audit data in one secure and easy-to-manage appliance. Access control is simplified with centrally managed authentication and access policies that integrate physical and IT security across your entire organization—around the globe. Imprivata streamlines access through strong authentication options like biometrics, proximity cards, smart cards, one-time-password tokens—even physical locations—with the convenience of single sign-on.

Imprivata OneSign bridges the gap between end-user productivity and security. It's built-in features support shared workstation workflows, enable One-Touch Desktop Roaming, solve unattended desktop problems and address transaction-level authentication.

With Imprivata, organizations can reduce the cost of demonstrating compliance with centralized, real-time tracking of employee access events. One-click reporting

quickly identifies password sharing, what applications users are authorized to access, and what credentials they are using.

Imprivata OneSign is available as a physical or virtual appliance. Both options are non-invasive and seamlessly integrate with your existing IT infrastructure. No changes are required to user directories, applications or physical access control systems—nor are they required for additional staffing or specialized skills. Imprivata OneSign virtual appliances are formatted using the industry standard Open Virtualization Format (OVF). Heterogeneous enterprises can be deployed with both virtual and hardware OneSign appliances.
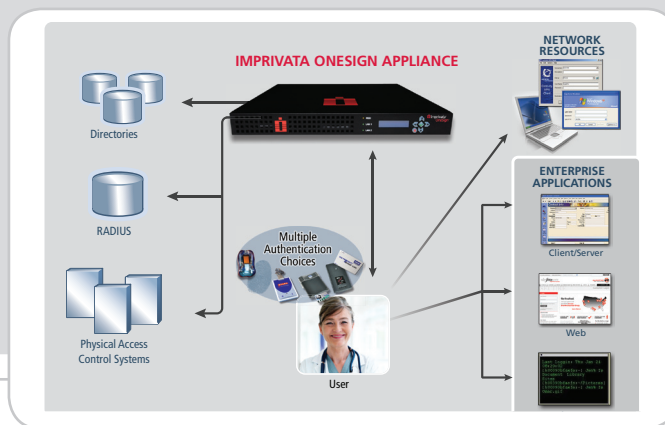


## TECHNICAL SPECIFICATIONS

Desktop Operating Systems
- Windows XP Professional, Windows XP embedded, XP Tablet, Windows Vista, Windows Server 2003, Windows Server 2008

Administration Console Requirements
- Microsoft Internet Explorer 7 or later running on supported Windows operating systems

Directories Supported
- Microsoft Active Directory, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID), Novell Netware, Novell eDirectory, IBM Tivoli
- Imprivata OneSign can provide single sign-on benefits for non-domain users who do not exist within the organization's corporate directory, such as temporary workers and partners

Strong Authentication Methods Supported
- Fingerprint biometrics, active and passive proximity cards, smart cards, many National Health and government ID cards, One-Time-Password, and USB tokens

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)
- All Win32 client-server or client applications on supported Windows OS
- Windows applications, Java applications
- Custom and legacy applications running on a supported Windows OS
- All clinical applications for healthcare including
  - Cerner
  - Eclypsis
  - Epic
  - GE Medical
  - Healthland
  - McKesson
  - Meditech
  - Siemens Medical
  - And many more...

## imprivata®

Securing employee access to desktops, networks, applications and transactions from around the world.

Belgium | Germany | Italy | Singapore | UK | USA

1 877 ONESIGN | 1 781 674 2700 | www.imprivata.com