



GET AWAY FROM PASSWORDS GET BACK TO CITIZENS



From the Executive Branch to the Judicial Branch, from Energy and Transportation to Public Safety and Health and Human Services, effectively serving the public requires that employees have unimpeded and secure access to disparate software applications and information systems—often from demanding locations, such as police cars out on community patrol.

However, too often the applications and information systems employees need to effectively serve their citizens are accessed and protected using only passwords. Passwords are weak in composition and easily hacked, shared amongst coworkers in violation of security policies, or lost and forgotten, resulting in possible disruption to vital public services—not to mention the password reset costs and resource burdens on IT helpdesks already stretched beyond capacity.

Securing access to public information is a critical issue for state and local agencies and many are adopting the best practices outlined by the National Institute of Standards and Technology (NIST) for federal computer systems, which call in part for agencies to implement a password policy that includes the use of strong passwords and single sign-on. Further, NIST guidelines recommend password policy be coupled with strong authentication (especially for remote access), such as a One-Time-Password (OTP) token or smart card. In fact, in an era of increased information sharing between local, state, and federal agencies, many federal-based information systems, such as the U.S. Federal Bureau of Investigation's (FBI) Criminal Justice Information Services (CJIS), now require strong authentication to access their systems.

For agencies seeking to enable their employees with secure and productive information access, the ideal solution would provide a centralized platform that strengthens user authentication for desktops and networks, streamlines application access, and simplifies the process of audit and reporting.

Imprivata OneSign® is that solution!

BENEFITS OF ONESIGN

- Reduces password administration and helpdesk costs
- Ensures compliance with strong password policies and security regulations
- Provides visibility into user access for authorized local and remote users
- Locks down all user network and application access upon departure from the organization
- Ensures network access for authorized local and remote users
- Relieves frustration and enhances user convenience and productivity

WHAT'S INSIDE THE BOX

SOLVING THE PASSWORD PROBLEM

Imprivata OneSign Single Sign-On® solves password management and application access issues. By single sign-on enabling ALL enterprise applications—without requiring custom scripting, modifications to existing directories, or disruptive changes to workflows—organizations can streamline, speed, and secure access to their corporate applications, improve employee productivity and satisfaction, and reduce the high costs of password management and reset call burdens on the IT helpdesk. With Imprivata OneSign Single-Sign On you can:

- Relieve frustration and enhance user convenience and productivity
- Reduce password administration and IT helpdesk costs
- Ensure compliance with strong password policies and security regulations
- Gain visibility into all user access activities across disparate applications

RAPID SINGLE SIGN-ON ENABLEMENT FOR ALL APPLICATIONS

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. OneSign's single sign-on (SSO) enablement simplifies the SSO profiling and does not require any scripting, modification of application code, or directory changes.

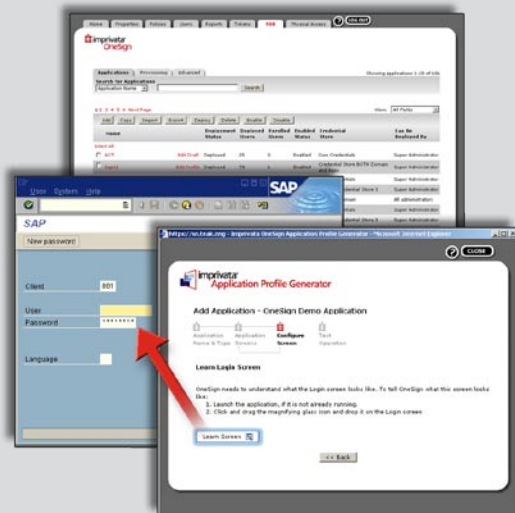
SELF-SERVICE PASSWORD RESET

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

STRENGTHENING INFORMATION SECURITY

Imprivata OneSign Authentication Management® enables flexible authentication management at the desktop, network, application, and transaction-level. By replacing weak Windows desktop, and remote VPN passwords with a broad range of strong authentication options— including finger biometrics, proximity cards, smart cards, government ID cards, OTP tokens, and an employee's physical location—organizations can centrally manage any combination of unique authentication modalities that best match employee roles and workflows. With OneSign Authentication Management you can:

- Centralize management of multiple strong authentication options within a single environment
- Ensure secure network access for authorized remote users
- Lock down all user network and application access upon departure from the organization
- Enable organizations to control and track data access at the individual user level





“OneSign works great in our heterogeneous IT environment, and the fingerprint readers are excellent. Best of all, our users are ecstatic.”

-Nelson Martinez Jr., Systems Support Manager, City of Miami Beach

BUILT-IN SUPPORT FOR MULTIPLE CARD TYPES

Imprivata OneSign natively supports active and passive proximity cards, Windows smart cards, building access cards, and government ID card technologies from leading vendors including:

- HID Crescendo, HID iClass, Casi-Rusco, Indala, Mitare, Ensure Xyloc, and others
- Supported desktop card readers include Ensure Xyloc readers, RF Ideas PCprox USB readers, and HID Omnikey USB readers.

BUILT-IN SUPPORT FOR FINGER BIOMETRICS

Imprivata OneSign’s built-in support for finger biometrics includes Dell, Lenovo, HP, Fujitsu, Motion, and other laptops with embedded UPEK or Authentec swipe sensors, as well as support for external UPEK and Authentec USB readers that you can mix and match on workstations or personal desktop machines.

Your end-user workflow is made easy – just one enrollment and your users can take advantage of biometrics in your organization.

BUILT-IN RADIUS HOST FOR REMOTE ACCESS AUTHENTICATION

The Imprivata OneSign platform includes a built-in RADIUS server to handle remote access authentication using DIGIPASS tokens by VASCO, RSA SecurID tokens, Secure Computing tokens, or passwords.

PHYSICAL/LOGICAL CONVERGENCE

OneSign Physical/Logical™ integrates network and building access systems to allow one, comprehensive, converged policy for allowing or denying network access based on a user’s physical location, role, and or employee status, for example: instantly deny all network access upon deactivation of an employee’s building ID badge.



SIMPLIFY COMPLIANCE REPORTING

Imprivata OneSign reduces the time and complexity of demonstrating compliance with data protection and privacy regulations. By tracking and consolidating disparate employee access events, agencies can rapidly respond to audit inquiries with real-time, aggregated views of when, how, and from where an employee gained network and application access. With the push of a button, Imprivata OneSign can report who is sharing passwords, what applications users are authorized to access, and what credentials they are using. When users separate from the agency, OneSign ensures that access — across all user accounts — is instantly revoked.

THE ONESIGN PLATFORM

The Imprivata OneSign Platform converges authentication and access management, seamlessly integrating strong authentication, application single sign-on, user provisioning, physical access control, and event reporting to enable centralized access policies that enforce every aspect of access across all users, rights, locations, and conditions.

Managed from a single, easy-to-use Web-based administrative console, the Imprivata OneSign platform is delivered in a purpose-built, highly secure, and self-contained hardened appliance. Non-invasive to your organization's existing IT infrastructure, Imprivata OneSign requires no changes to user directories, applications, or physical access control systems, and does not require additional staffing or specialized management skills.

TECHNICAL SPECIFICATIONS

Desktop Operating Systems

- Windows 2000 Pro, Windows XP Professional, Windows XP embedded, Windows Vista, Windows Server 2000, Windows Server 2003, Windows Server 2008

Administration Console Requirements

- Microsoft Internet Explorer 6.1 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 LDAP
- If needed, single sign-on benefits can be extended to users who do not exist within the organization's core directories, e.g., visiting physicians or students, through a OneSign directory

Strong Authentication Methods Supported

- Fingerprint biometrics, active and passive proximity cards, smart cards, many National Health and ID cards, One-Time-Password, and USB tokens

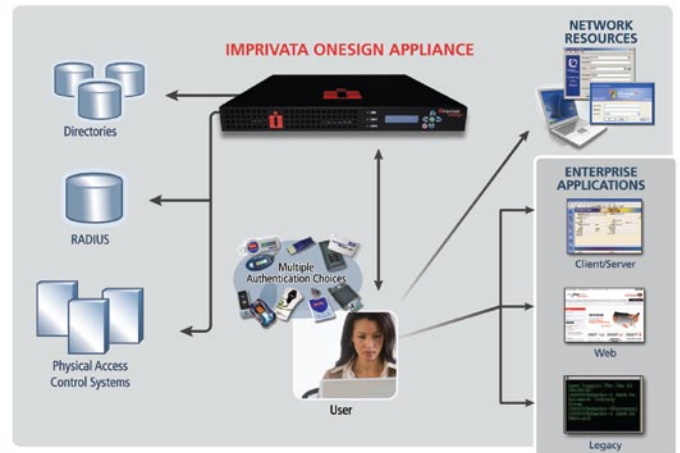


Bringing secure employee access management to companies around the world from our offices in:

Belgium | Germany | Italy | Singapore | UK | USA

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

Designed for flexible and rapid enterprise deployment and easy integration, Imprivata OneSign's appliance-based solution dramatically minimizes implementation time, infrastructure needs, and installation costs—accelerating your return on investment and lowering your ongoing support costs.



Physical Access Control Systems Supported

- AMAG - Symmetry™
- Honeywell - Pro-Watch®
- Lenel Systems International - OnGuard®
- Nedap - AEOS®
- S2 Security - NetBox™
- Software House® - C•CURE®

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

Appliance

- Pair of ready-to-use, redundant 1U rack-mountable appliances. More appliances can be added for disaster recovery or to scale for large and/or geographically dispersed enterprises