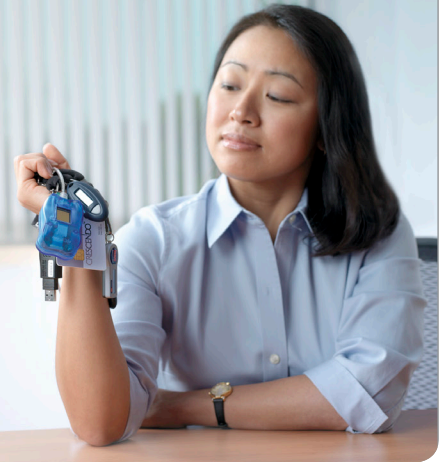




## USERS NEED DIFFERENT STRONG AUTHENTICATION OPTIONS, BUT MANAGING THEM ALL IS THE CHALLENGE.



### YOU NEED STRONG AUTHENTICATION BUT NOT THE HEADACHES AND COMPLEXITY

Security experts agree that the best way to protect your organization's information assets and comply with data protection regulations is to deploy strong authentication—two forms of proof before access can be granted—to ensure authorized access. This proof can come in many forms, but generally falls into one of four categories: “something you know” (a personal pin or a familiar word), “something you have” (security token or access card), “something you are” (a unique personal feature, such as a fingerprint), or “somewhere you are located” (linking a person's network access to a particular zone within a workplace).

However, what if you have multiple types of users, access privileges, and degrees of information sensitivity? You could deploy and manage multiple strong authentication solutions throughout your enterprise, but this could be a complex and costly endeavor, requiring multiple redundant servers, communication paths, management consoles, client-side agents, and configuration back-ups. Maintenance could be a nightmare, because these interconnected components can change independently, increasing your exposure and posing a security risk.

### STRONG AUTHENTICATION DELIVERS GREATER PROTECTION

Imprivata OneSign® Authentication Management takes the complexity and cost out of [strong authentication](#) implementation by providing a single authentication management solution that supports most strong authentication options and enforces secure and compliant employee access to networks and applications, both local and remote. Imprivata OneSign Authentication Management helps combat weak network logons by

replacing Windows and remote access VPN passwords with your choice of a broad range of strong authentication options, including integrated management for finger biometrics, active and passive proximity cards, smartcards, and One-Time-Password and USB tokens.

With Imprivata OneSign Authentication Management, you can economically deploy comprehensive, scalable, and high-performance authentication management, whether users are accessing the network locally or via VPN—or even while working offline. Imprivata OneSign records all user events in a centralized log file, which provides the reporting trail required for regulatory auditing and compliance purposes that can be centrally viewed and exported to reports.

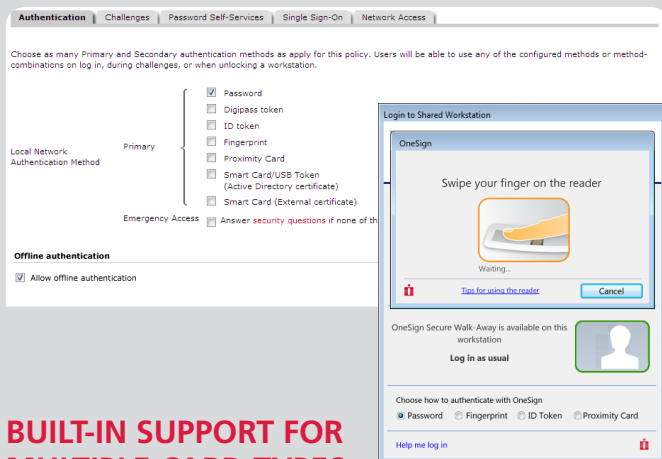
### BENEFITS OF IMPRIVATA ONESIGN AUTHENTICATION MANAGEMENT

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

# WHAT'S INSIDE THE BOX

## BUILT-IN SUPPORT FOR FINGER BIOMETRICS

Imprivata OneSign supports Dell, Lenovo, HP, Fujitsu, Motion, and other laptops with embedded UPEK or Authentec swipe sensors, as well as external UPEK and Authentec USB readers that may be mixed and matched on workstations or personal desktop machines. With just one enrollment, your users can authenticate to the network with a simple swipe or scan. Imprivata OneSign then matches the user's fingerprint against all known fingerprints using one-to-many matching.



## BUILT-IN SUPPORT FOR MULTIPLE CARD TYPES

Imprivata OneSign natively supports active and passive proximity cards, Windows smart cards, building access cards, and many National Health 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

## IMPRIVATA ONESIGN VDA™—IMPROVED END-USER WORKFLOW

Imprivata OneSign Virtual Desktop Access™ (VDA) enables organizations to realize the cost and efficiency benefits of desktop virtualization by giving users fast and secure desktop access to applications. One-Touch Desktop Roaming and location awareness enables desktops to follow users throughout the office, making the data they need available to them wherever they are with just the touch of a finger or the tap of a proximity card.

Imprivata OneSign can be configured to be fully location aware, meaning application, default printer and user privileges are configured dynamically based

on the particular workstation being accessed by the clinician. Imprivata OneSign complements desktop virtualization from VMware View™ and Oracle's Sun Ray, by adding the capabilities to enable secure roaming including strong authentication, single sign-on (SSO), session management and location-aware desktop personalization and customization.

## BUILT-IN SUPPORT FOR DIGIPASS BY VASCO

Imprivata OneSign Authentication Management has built in support for DIGIPASS by VASCO, token enrollment, and policy management, allowing organizations to replace network passwords with two-factor authentication that secures access for users—on the local network, offline and logging onto their laptops, or accessing network resources via VPN.

## 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.

## FIPS 140-2 COMPLIANCE

Imprivata OneSign's industry leading strong authentication solution is now also available with an embedded hardware security module to provide the highest security required to meet FIPS 140-2 mandate. This packaging option will be marketed to government sectors, where security mandates including the U.S. Code of Federal Regulations (CFR), the Homeland Security Presidential Directive (HSPD)-12 and Federal Information Processing Standard (FIPS) Publication 201 imposes strict requirements.

## ONESIGN SECURE WALK-AWAY™—AUTOMATIC DESKTOP LOCK

OneSign Secure Walk-Away™ (SWA) closes a critical security gap in the protection of confidential patient information records by automating the process of securing the desktop when a user 'walks away'. Imprivata OneSign SWA uses intelligent computer vision technology with active presence detection to secure unattended desktops without changing end-user behavior. This removes the security burden from the user and reduces the time and frustration associated with logging on/off of applications.



“Imprivata OneSign has done more for us than just logging users into apps. It’s a foundation that has enabled fingerprint biometrics, two-factor authentication, and proximity security.”

- Frank Fear, CIO, Memorial Healthcare

## ONESIGN FASTPASS™—ONE-TOUCH LOGIN TO ANY DESKTOP

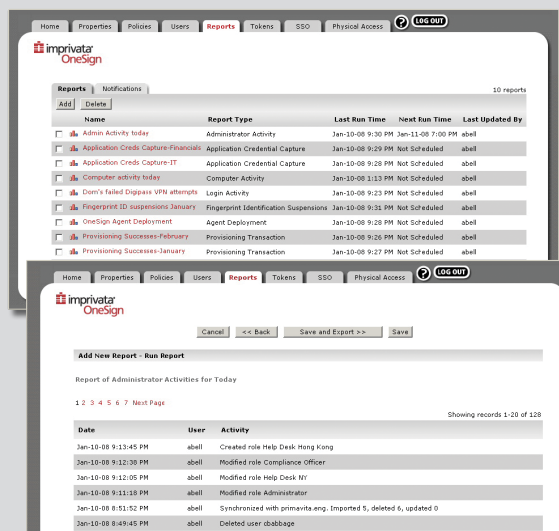
OneSign FastPass provides fast and secure desktop access with the simple touch of a user’s fingerprint or proximity ID card without having to type their Windows username and password every time they log on. OneSign FastPass provides a second factor authentication ‘grace period’ during which users may access any desktop without the need to enter a second factor such as a PIN or password until their ‘grace period’ expires.

## PHYSICAL/LOGICAL CONVERGENCE

Imprivata 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, e.g., instantly deny all network access upon deactivation of an employee’s building ID badge.

## APPLICATION TRANSACTION-LEVEL STRONG AUTHENTICATION

Imprivata OneSign ProvelD leverages Imprivata OneSign’s strong authentication services to positively identify a user at any point in the application workflow. Examples include banking environments where positive identification of a user is required prior to execution of a financial transaction and healthcare environments where positive identification of a user is required at the point of a drug disbursement.



## MONITORING AND CONSOLIDATED REPORTING

Imprivata OneSign records all local and remote network authentication and application access events in a centralized database. A push of a button provides a standardized report in real-time with an aggregated view of who, when, how, and from where an authorized user gained access to the network. This ensures rapid responses to audit inquiries that would otherwise require manual viewing and collation of independent system logs. Add the Imprivata OneSign Single Sign-On module and you can incorporate reporting on user access events to applications, as well.

## THE IMPRIVATA ONESIGN PLATFORM

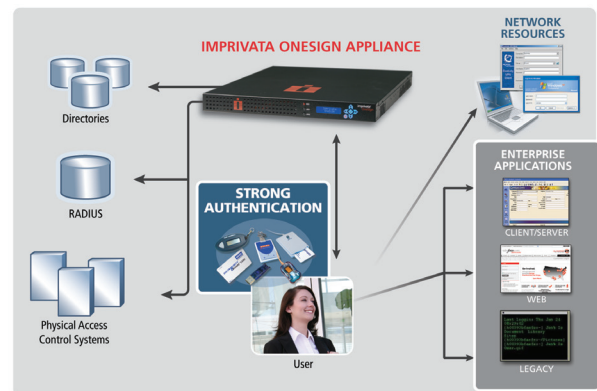
Imprivata OneSign is an identity and access management platform that integrates **user authentication**, user access, **password management** and aggregated audit data in one secure and easy-to-manage appliance. Access control is simplified with centrally managed authentication and access policies that 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. Its 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, 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 LDAP
- 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

### Physical Access Control Systems Supported

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

### 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



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](http://www.imprivata.com)

Copyright © 2010 Imprivata, Inc. All rights reserved. Imprivata and OneSign are registered trademarks of Imprivata, Inc. in the U.S. and other countries. The Application Profile Generator and OneSign Agent are trademarks of Imprivata, Inc. All other trademarks are the property of their respective owners

MKT-DS-AM-Ver4.0-09-2010.