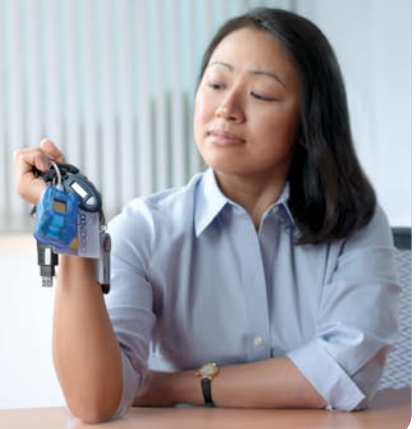




USERS NEED DIFFERENT STRONG AUTHENTICATION OPTIONS, BUT MANAGING THEM ALL IS THE CHALLENGE.



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).

But 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.

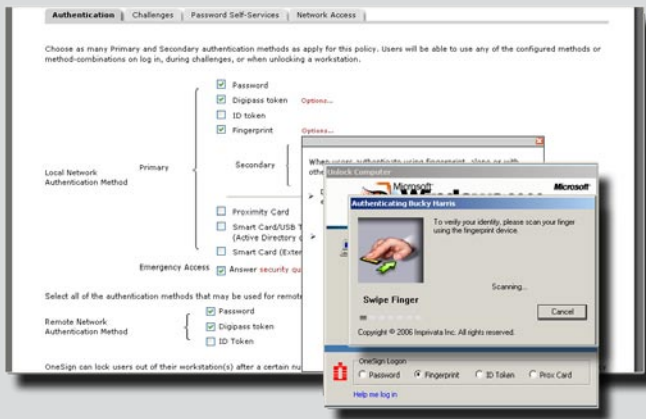
BENEFITS OF IMPRIVATA ONESIGN AUTHENTICATION MANAGEMENT

- 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'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 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

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.

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.



“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

APPLICATION TRANSACTION-LEVEL STRONG AUTHENTICATION

Imprivata OneSign ProveID 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 top screenshot displays the 'Reports' section of the Imprivata OneSign interface. It includes a table with the following data:

Name	Report Type	Last Run Time	Next Run Time	Last Updated By
Admin Activity Today	Administrator Activity	Jan-10-08 9:30 PM	Jan-11-08 7:00 PM	abell
Application Credentials Capture-Financials	Application Credential Capture	Jan-10-08 9:29 PM	Not Scheduled	abell
Application Credentials Capture-IT	Application Credential Capture	Jan-10-08 9:28 PM	Not Scheduled	abell
Computer activity today	Computer Activity	Jan-10-08 9:13 PM	Not Scheduled	abell
Dom's failed Digipass VPN attempts	Login Activity	Jan-10-08 9:23 PM	Not Scheduled	abell
Fingerprint ID suspensions-January	Fingerprint Identification Suspensions	Jan-10-08 9:31 PM	Not Scheduled	abell
OneSign Agent Deployment	Agent Deployment	Jan-10-08 9:28 PM	Not Scheduled	abell
Provisioning Successes-February	Provisioning Transaction	Jan-10-08 9:26 PM	Not Scheduled	abell
Provisioning Successes-January	Provisioning Transaction	Jan-10-08 9:27 PM	Not Scheduled	abell

The bottom screenshot shows a detailed report titled 'Report of Administrator Activities for Today'. It includes a table with the following data:

Date	User	Activity
Jan-10-08 9:13:45 PM	abell	Created role Help Desk Hong Kong
Jan-10-08 9:12:30 PM	abell	Modified role Compliance Officer
Jan-10-08 9:12:05 PM	abell	Modified role Help Desk NY
Jan-10-08 9:11:18 PM	abell	Modified role Administrator
Jan-10-08 8:51:52 PM	abell	Synchronized with primavita.eng. Imported 5, deleted 6, updated 0
Jan-10-08 8:49:45 PM	abell	Deleted user cballbage

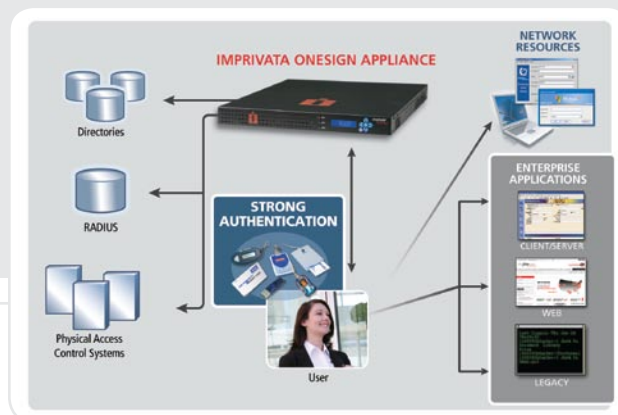
THE ONESIGN PLATFORM

Imprivata OneSign Single Sign-On is a module within the Imprivata 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 policies that enforce every aspect of employee access across all users, rights, locations, and conditions.

Managed from a single easy-to-use web-based administrator 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.

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



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
- 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

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



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

Copyright © 2009 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-Ver3.0-0909.