Imprivata OneSign Authentication Management

Benefits

- 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

Secure, Simple Access for Users

Protecting organizational assets, complying with data protection regulations all while providing easy access for end users can be a challenge. By deploying strong authentication—two forms of proof before access can be granted—secure, simple access is a given. Strong authentication 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.

Simplified Management For IT

Imprivata OneSign® Authentication Management takes the complexity and cost out of strong authentication implementations by providing a single authentication management solution that supports a broad range of 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 log-ons by replacing Windows and remote access VPN passwords with your choice of a broad range of strong authentication options, including integrated management for fingerprint biometrics, active and passive proximity cards, smartcards, one-time passwords, USB tokens and out-of-band phone-based authentication.

With Imprivata OneSign Authentication Management, organizations 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 audit trail required for regulatory auditing and compliance purposes that can be centrally viewed and exported to reports.

Shared workstations can be frustrating, however, with Imprivata OneSign a simple tap of a badge or swipe of a fingerprint unlocks or locks any workstation.

Broad Strong Authentication Support

Imprivata supports a broad range of authentication options allowing for a single point of management for two factor authentication administration and authentication enrollment enabling administrators and users to enroll cards and fingerprints—simplifying roll-out, replacement cards and new user support.

Fingerprint Identification

Imprivata OneSign identifies and authenticates with the swipe of a fingerprint—no need to enter a username.

No Click Access to Physical or Virtual Desktops and Applications

Imprivata OneSign Virtual Desktop Access builds on the benefits of desktop virtualization by streamlining access to roaming desktops providing No Click Access® to virtual desktops with just the tap of a badge or swipe of a fingerprint. Imprivata OneSign Virtual Desktop Access complements desktop virtualization solutions such as VMware View, Citrix XenDesktop and Oracle Sun Ray.

Shared Workstations, Fast User Switching

Shared workstations can be frustrating, however, with Imprivata OneSign a simple tap of a badge or swipe of a fingerprint unlocks or locks any workstation allowing for fast user switching between multiple, concurrent Windows desktops, as well as secure fast user switching on top of a generic kiosk desktop.

Automatic Desktop Locking and Re-authentication

Automatically lock desktops and re-authenticate users with Imprivata OneSign Secure Walk-Away® which uses a combination of active user presence detection and facial recognition to automatically secure the desktop when the user moves away and re-authenticates them on return—removing any risk of exposing corporate assets.

Anywhere Authentication and Single Sign-On

OneSign Anywhere® enables secure authentication for users at any time and from any location. The OneSign Anywhere agentless technology gives users the flexibility to use any device—home computer, iPad or smartphone—without the need to remember and input multiple usernames and passwords. Imprivata's partnership with PhoneFactor allows for two-factor out-of-band authentication via an automated phone call or text message.

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 option supports 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.

Self-Service Password Reset

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

Transaction Level Strong Authentication

Imprivata OneSign ProveID provides secure, seamless access when authenticating, or re-authenticating at any point during the application workflow such as in banking environments where positive identification of a user is required prior to execution of a financial transaction.

Independent Software Vendors (ISVs) and Hardware Vendors (IHVs) can utilize the ProveID APIs to embed authentication and re-authentication within their solutions. The integration is done through a partnership between Imprivata and ISVs/IHVs which includes participation in a Developers Program and certification of the solutions by Imprivata.

Consolidated Reporting

Imprivata OneSign records all local and remote network authentication 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.

Technical Specifications

http://www.imprivata.com/technical_specifications

Imprivata OneSign records all local and remote network authentication access events in a centralized database.

imprivata®

About Imprivata

Imprivata is a leading provider of authentication and access management solutions for the healthcare industry. Imprivata's single sign-on, authentication management and secure communications solutions enable fast, secure and more efficient access to healthcare information technology systems to address multiple security challenges and improve provider productivity for better focus on patient care.

Over 2 million care providers in more than 1,000 healthcare organizations worldwide rely on Imprivata solutions. Imprivata is the category leader in the 2012 and 2013 Best in KLAS Software & Services Report for SSO, and SSO market share leader according to HIMSS Analytics.

For further information
please contact us at:
1 781 674 2700
or visit us online at
www.imprivata.com

Offices in:
Lexington, MA USA
Santa Cruz, CA USA
Uxbridge, UK
Paris, France
Nuremberg, Germany
Den Haag, Netherlands

MKT-DS-AM-Ver1-0214