



that is changing Authentication Management

With the advent of stringent government and industry security regulations, organizations are looking for a way to replace the vulnerable Windows logon password with a stronger form of authentication. So far, solutions have been complex and expensive.

Enter **Imprivata OneSign® Authentication Management**. For organizations that need to increase user access security to Microsoft Windows environments, OneSign Authentication Management replaces network passwords with two-factor strong authentication, regardless of whether users are online and connecting to the corporate network or offline and logging onto their laptop.

For companies of all sizes, OneSign Authentication Management simplifies the cost and complexity of managing network access security across a highly distributed enterprise. It is the industry's most powerful and innovative authentication management solution.

➔ Radically Easy

Out-of-the-Box Appliance

OneSign is shipped as a redundant appliance pair, pre-installed and ready to go for quick and easy deployment. There is no additional hardware or software to buy, install, integrate, or maintain. A distributed architecture allows multisite deployment for business continuity, availability, and disaster recovery supporting an unlimited number of users.

Single Authentication Management Platform

OneSign makes authentication management—even token

enrollment—flexible and easy. Deploy secure network access within hours without changing existing user directories. Policies are centrally managed and can be transparently applied in minutes. Users remain productive with minimal day-to-day management, and the user desktop experience is unchanged.

Easier Compliance and Reporting

Built-in monitoring, logging, and reporting tracks which users logged in and when, allowing organizations to strengthen security policies and demonstrate regulatory compliance.

➔ Simply Smart

Choice of Strong Authentication – Online or Offline

Windows passwords are the weakest link in your enterprise security. OneSign Authentication Management is flexible, providing out-of-the-box support for a wide range of strong authentication options, including easy administration of One-Time Password (OTP) tokens, active/passive proximity cards, smart cards, USB tokens, and finger biometrics—making for a more secure front door.

Integrated VASCO® DIGIPASS® Token Management

With an embedded RADIUS host and a VACMAN Controller from VASCO Data Security, OneSign enables customers to quickly set

up, deploy, and manage any type of DIGIPASS token—for both remote and local network authentication.

Seamless Upgrade to Single Sign-On and Integrated IT/Building Access

The OneSign appliance is a complete and comprehensive platform for converged identity and access management. With a simple license key, customers can extend OneSign Authentication Management to seamlessly enable single sign-on to enterprise applications and/or converged security policy with leading physical access security vendors for “location-based” authentication.

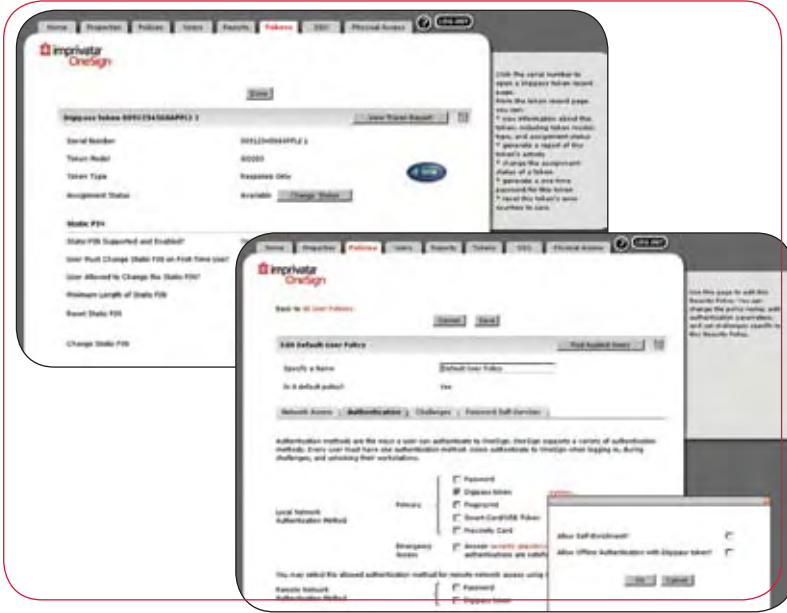
➔ Uniquely Affordable

Lowest Cost Two-Factor Authentication

OneSign's fast implementation, quick user adoption, and built-in support for multiple authentication methods delivers instant cost savings—and immediate financial return. As a self-contained

appliance, OneSign Authentication Management delivers all the functionality needed to effectively implement and manage network authentication. There is nothing else to buy and no costly integration.

Simple Way to Manage the Entire Authentication Management Process



Application Transaction Level Strong Authentication



OneSign's ProvelD capability allows an application to leverage OneSign's strong authentication services to positively identify a user at any point in the application workflow. Examples of ProvelD in use include a banking environment where positive identification of a user is required prior to executing a financial transaction, and a healthcare environment where positive identification of a user is required at the point of drug disbursement.

Imprivata OneSign Authentication Management provides a radically easy, simply smart, and uniquely affordable enterprise network authentication solution that delivers increased security at the Windows logon.



OneSign & DIGIPASS

- OneSign Authentication Management includes integrated VASCO token management —no additional servers needed.
- Customers can enroll ANY DIGIPASS token for network authentication use with OneSign. It's quick. It's easy. There's nothing else to buy.



TECHNICAL SPECIFICATIONS

Administration Console Requirements

- IE 6.0 or later running on Windows 2000, Windows XP Professional or XP embedded, Windows Server 2000, Windows Server 2003.

Client Systems Supported

- Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003, Windows Vista, Windows XP Tablet.

Directories Supported

- Microsoft Active Directory 2000 / 2003 Server, NT 4.0 Domain, Sun ONE Directory Server 5.0, Oracle Internet Directory (OID) 10g, Novell Netware 5.1 running NDS 8.0 or later, Novell eDirectory 8.0, IBM Tivoli LDAP.

Strong Authentication Methods Supported

- OTP Tokens, proximity cards, smart cards, USB token, and finger biometrics.

Appliance

- Pair of ready-to-use redundant 1U rack-mountable servers. Failover is included. O/S is Novell's SUSE® LINUX Enterprise 9.



www.imprivata.com • sales@imprivata.com • 1 877 ONESIGN

Corporate Headquarters

10 Maguire Road
Building 4
Lexington, MA 02421
t 781 674 2700
f 781 674 2760

Imprivata EMEA

Forsyth House, 77 Clarendon Road
Watford, Herts WD17 1LE
United Kingdom
t +44 (0)1923 813 511
f +44 (0)1923 813 501

Imprivata APAC

#01-03 60 Cambridge Road
Singapore 219757
t +65 82 004 840