



The BOX



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.

OneSign Authentication Management simplifies the cost and complexity of managing network access security for companies of all sizes. It is the industry's most powerful and innovative authentication management solution.

➔ Radically Easy.

Out-of-the-box-Compliance

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. Additionally, OneSign includes seamless real-time failover and can be restored from a back-up within minutes for disaster recovery.

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, 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 solution for enterprise authentication 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.

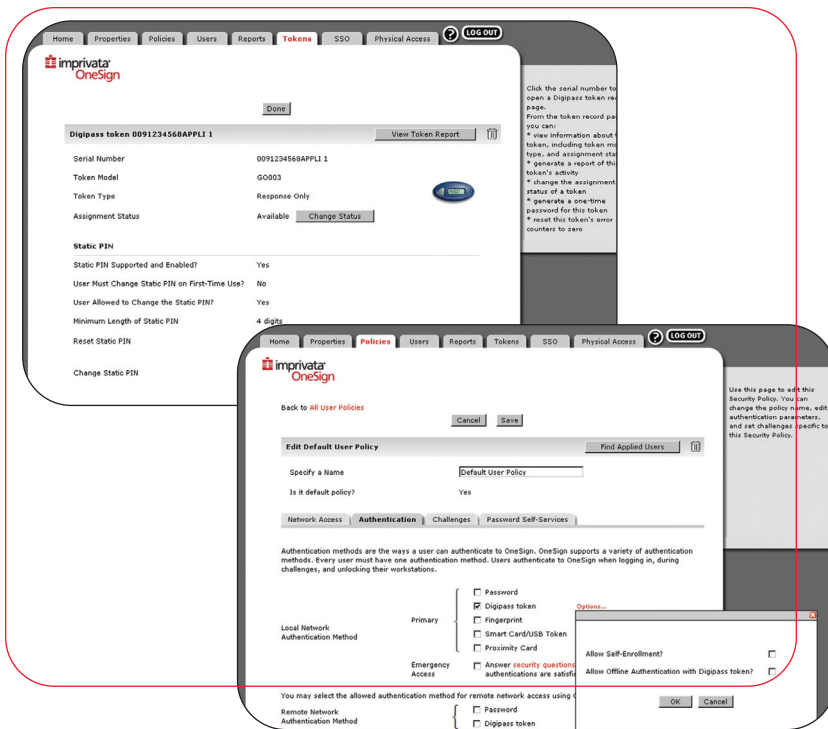
➔ Uniquely Affordable.

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

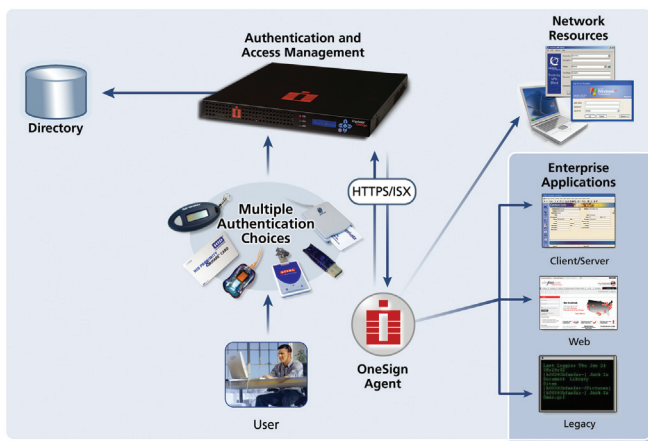


OneSign & Digipass

- 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.



OneSign Authentication Management Enrollment and Deployment



The OneSign Appliance provides flexible on-ramps to enterprise authentication and access management. Customers beginning with OneSign Authentication Management can seamlessly enable single sign-on to enterprise applications, and/or unified IT/Building access—with just an upgrade of the license key.

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. The OneSign Appliance removes complexity, providing convenience for companies of all sizes.

To learn more, visit www.imprivata.com, contact us at sales@imprivata.com, or call 877-OneSign (877-663-7446).



Corporate Headquarters

10 Maguire Road, Building 2, Lexington, MA 02421
v 781 674 2700 f 781 674 2760

Imprivata EMEA

Forsyth House, 77 Clarendon Road
Watford, Herts WD17 1LE, United Kingdom
v +44 (0)1923-813511 f +44 (0)1923-813501

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

- IE 5.5 or later running on Windows 2000 SP3, Windows XP Professional SP1 or XP embedded SP1, Windows Server 2003.

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.