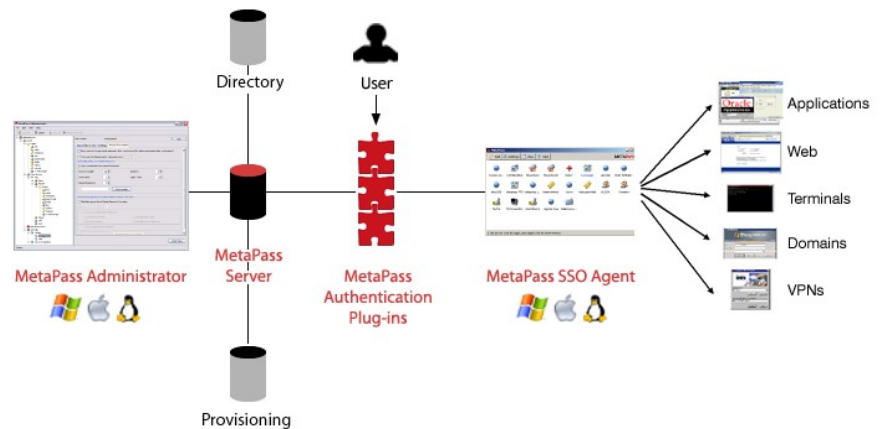


MetaPass SSO Version 4.0

Universal Enterprise Single Sign-On

The Single Sign-On Challenge

Enterprise Single Sign-On (E-SSO) allows computer users to access multiple secure systems without having to remember and enter multiple passwords. It also allows administrators to control who has access to what in the organization, audit and report access events. The purpose of E-SSO is to dramatically increase security and productivity, ensure regulatory compliance, while reducing helpdesk costs. It is supposed to be the “magic pill” to fix all password-related problems. However, most E-SSO implementations have fallen short on this promise because it is technically very difficult to make it work. With so many applications on the market developed in multiple computer languages and platforms, such as web, desktop, client-server, terminal/mainframe, standard and home-grown... there is no common interface to integrate them all. How can you possibly automate the login process with so many different kinds of applications? Old-generation E-SSO solutions run only on Windows and therefore are highly dependent on this operating system. They use internal functions (Windows APIs) to push credentials, such as IDs and passwords, to applications. While this method is technically easy and works in a number of cases, it also doesn't work in many others.. In order to integrate in all situations, a lot of custom work is necessary, without even guarantee of success. In fact, it rarely works with everything: generally single sign-on is merely “reduced sign-on” and users still have a number of passwords to type and remember. Worse, maintenance is a real nightmare, because the internal



functions of the OS are constantly changing (patches, service packs...), and the E-SSO may not continue to work reliably with certain applications. The problem has not been solved... until now.

Why Multiplatform is Critical

MetaPass takes a completely new approach to integrate with your applications. The MetaPass' patent-pending technology runs independently on Windows, Mac OS, and Linux, both at the client and server levels. Rather than being OS-dependent, it operates at a higher abstraction layer than running applications, and pushes credentials directly to them without going through internal OS functions.

Universal Integration with all your Applications

As a result, MetaPass is totally system-agnostic and works with any application, no matter what it looks like, how it behaves or what version it is.. This approach is revolutionary in the sense that it finally enables E-SSO to work.

The MetaPass Technology

The secret of the patent-pending MetaPass technology lies in virtualizing the user interface, making it completely independent of the application and even the operating system. MetaPass does not rely on Windows-specific commands (APIs), nor does it need to parse HTML code, nor does it even care in what programming language (C++, Java, Flash...) the applications are developed in. It treats and interacts with all types of applications (web, client-server, terminal, etc) the same way, operating at an abstraction layer that is above (“meta”) running applications. The result is a remarkable level of compatibility with any of your applications, standard or home-grown, now and in the future.

No pre-defined templates

Because MetaPass virtualizes the user interface and becomes independent on the applications, there is no need for pre-defined applications scripts or templates that inevitably expire when applications get updated. As a result, not only is MetaPass much easier to integrate, but also to maintain.

One-Click Login

From the user's standpoint, it could not be easier. The user only needs to authenticate once to MetaPass, using a master password, or the OS authentication (e.g. Windows Logon), or a strong authentication device such as a smart card or a fingerprint reader. Once authenticated, the user just needs to click on an icon to log onto a system. MetaPass does the rest. This is called "One-Click Login", and this is the only thing the user needs to do to access any system.

Central Administration

IT Administrators use the MetaPass Administration Console and Server software to manage users across the organization. This software is not only used to configure MetaPass to interface with your applications, but it also connects to your directory, allowing you to associate applications with users or groups of users. For example, you may decide that your whole Marketing department should have access to 12 websites, 5 applications, and 2 servers. You can accomplish that with just with a few drag and drop operations, and a push of the "Synchronize Users" button. Users receive their access rights and can instantly access those systems. Users' rights can be updated any time, in real time. This can be done by group of users, or individually per user when granularity is important. The MetaPass Administration Console and Server also allows for setting up user policies, i.e. what users can and cannot do with MetaPass, how they authenticate, how and where passwords are encrypted and stored, etc. It also provides functions to automatically change passwords from whatever the users chose to long, strong, randomly-generated passwords that are much more difficult to crack. At some point, you may decide to even hide passwords from users. This way, they will not write them down or share them with others.

Enhanced Security

The MetaPass solution is end-to-end encrypted using an SSL secure channel between the Administrator and Users. Then, data is encrypted a second time to store credentials locally, in smart cards, in a server, in a database, or in

a directory. In addition to where the credential is stored, you also choose the encryption method such as the AES encryption standard.

No infrastructure change

Because of its "meta", or universal, approach, MetaPass works instantly without the need for you to change anything in your existing applications or infrastructure. MetaPass adapts to your infrastructure, not the other way around.

Distributed Architecture:

No single point of failure

Rather than relying on a centralized system to store and/or pass credentials, MetaPass is completely decentralized. The MetaPass Administration Server is used only to update users, who can use MetaPass even when disconnected or if the server goes down.

Strong Authentication

For an added level of security, MetaPass supports multiple authentication systems such as smart cards, tokens, biometrics, proximity badges, directory/domain authentication.

Better yet, the configuration of those devices is dramatically simplified with a built-in editor where you connect components together visually, without writing a single line of code. For example, you may decide to store credentials in a SQL database, and encrypt the data with keys that are stored in users smart cards. Even though the SQL database and the smart cards are manufactured and supported by different vendors, MetaPass makes them talk to each other for a seamless integration. You may decide on different types of authentication for different types of users (e.g. regular, power users, etc). MetaPass automatically builds installers that contain all drivers, configuration files, etc. and are pushed from a centralized location for easy deployment.

Deployment is a Snap

Usually, Enterprise Single Sign-On is a nightmare to deploy because of the variety of systems and of users. Again, MetaPass has dramatically simplified this process and allows for fast

deployment to virtually any number of users. Several options are available, such as using an MSI or the built-in MetaPass deployment tool. Similarly, updating users is fast and simple. With a single click, all users can receive, transparently and through the network, software updates.

Storage and Backup

You choose where you want to store data:

- Hard drive
- Smart card
- Server
- Database
- Directory
- and more

You also choose your favorite encryption algorithm, and MetaPass takes care of the rest.

MetaPass comes with an automatic and secure backup functionality so you can rest assured that even if the worst happens, your data is safe.

Logging and Event Reporting for Compliance

Regulatory compliance requires you to audit users: who accessed what, when, etc. MetaPass allows you to keep track of all user events related to accessing their systems. You then export reports used for regulatory compliance.

Directory Integration

Leverage your directory and use it for single sign-on. MetaPass integrates seamlessly with most directories in the market, without the need for you to change the schema.

Kiosk Mode

When users share computers, they need to be able to rapidly switch from one account to another. MetaPass provides a "kiosk mode" that not only logs users onto their applications, but also logs them off automatically when an event is triggered (time out, user switch, etc).

Automatic Password Change

In addition to automatically logging users on and off all of your applications, the universal MetaPass technology is also used to automatically change passwords for all your applications, not just a few. This is an important functionality

because this is what truly increases the security of your network. For each of your applications, you define a password-change policy (e.g. every 30 days, 18 characters mixing number and letters, etc), and MetaPass does it automatically. You may decide to change passwords more often than what applications require.

Multi-Language

MetaPass is completely Double-Byte compliant and is currently available in:

- English
- German
- Spanish
- French
- Italian
- Chinese
- Japanese

MetaPass seamlessly integrates with applications and push credentials in any of these languages, such as Kanji passwords.

Platforms

- Windows 2000, 2003, XP, Vista
- Mac OS X on PowerPC and Intel
- Linux

Browsers

- Mozilla Firefox
- Internet Explorer
- Netscape
- Safari
- AOL
- Opera
- and more

Applications

- Native Windows
- Native MacOS
- Native Linux
- Java
- .NET
- SAP
- Citrix (published or not)
- Flash
- and more

TTY and Mainframe Applications

- Telnet
- 3270 (IBM Mainframe)
- SSH
- 5270 (AS/400)
- Virtually any emulator such as WRQ

Strong-Authentication Methods

- Smart cards
- Tokens
- Biometrics
- Proximity badges
- Directory/domain authentication

Networking and VPN

- Cisco
- Checkpoint
- iPass
- Nortel
- and more

System Requirements for MetaPass SSO

MetaPass Server

- Windows 2000 (Server or Workstation)
- or Windows 2003 Server
- or Windows XP Professional Edition (Server or Workstation)
- or Windows Vista
- or Red Hat Linux Enterprise Edition 4 or later
- or SUSE Linux 9 or later
- or Mac OSX 10.3 or later on Intel or PowerPC processor
- Minimum 1GB free space on the hard drive
- Minimum 512MB RAM

MetaPass Administrator

- Window 2000 (with SP4)
- or Windows XP Professional Edition (with SP1 or SP2)
- or Windows Vista
- or Red Hat Linux Enterprise Edition 4 or later
- or SUSE Linux 9 or later
- or Mac OSX 10.3 or later on Intel or PowerPC processor
- Minimum 500MB free space on the hard drive
- Minimum 512MB RAM

MetaPass Desktop

- Window 2000 (with SP4)
- or Windows XP Professional Edition (with SP1 or SP2)
- or Windows Vista
- or Red Hat Linux Enterprise Edition 4 or later
- or SUSE Linux 9 or later
- or Mac OSX 10.3 or later on Intel or PowerPC processor
- Minimum 80MB free space on the hard drive
- Minimum 512MB of RAM

MetaPass, Inc.

1230 Oakmead Parkway, Suite 306

Sunnyvale, CA 94085

USA

+1 (408) 907-3991 Voice

+1 (408) 716-2689 Fax

www.metapass.com