

### 3 Reasons to Implement FastPass Password Manager:

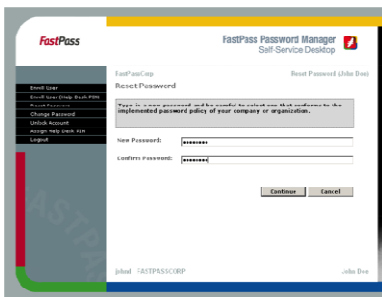
- Promotes user productivity
- Reduces IT Service Desk workload and cost
- Enhances security

### Proven Return on Investment

According to Forester, the average total internal cost of each password-reset call to Service Desk is \$100. 20–50% of all calls to Service Desk are related to password problems. Organizations that deploy the FastPass Solution eliminate these calls, allowing organizations to reassign support staff to other issues.

### Proven Successful

The FastPass Solution is used by thousands around the world. From medium sized companies to large Enterprise organizations and Service Providers – FastPass is helping users in all industries helping themselves.



FastPass Self-Service client

## Enterprise Password Management

When users have many passwords to remember, with complex compositions and frequent changes, they tend to forget their passwords – or write them on sticky yellow labels! This is either an economic headache or a dangerous breach of security!

Enterprises today demand Password Management solutions that increase productivity, strengthen security and improve service for end-users. Large organizations require that solutions are flexible and dynamic enough to reflect all the different options necessary in complex environments. Organizations are used to making compromises between IT security and cost, but FastPass Enterprise allows organizations to implement password policies according to the security impact of their IT resources and still benefit from end-user self-service, which leads to substantial cost savings at the Service Desk and improved service for the end-user!

FastPass Password Manager is a web-based solution that enables users with forgotten passwords or locked accounts to solve these issues on a 24/7 self-service basis, eliminating the need for support from the IT Service Desk. Users authenticate by answering personal questions, entering PINs or any other supported authentication method. Security administrators can configure single- or multi-factor authentication profiles. These profiles can be applied to users based on their network connection, making FastPass Password Manager a robust and very secure solution.

## User Self-service from both internal and external networks!

Users can easily reset their own password without any introduction to or training with FastPass. You can configure FastPass to meet your exact security requirement for each user group. Some users may be allowed to reset passwords based on simple authentication, whereas other user groups (High-risk users) may require stronger authentication. The authentication for the individual user may even vary according to the time of day or location and thus dynamic authentication is required. For strong authentication, Fast Pass can send a one-time PIN code to a user's mobile phone, in addition to the normal process of answering private questions. When a user is locked, due to too many attempts to logon, the user can unlock his account with FastPass and the password can be reset so he can get back to work straight away. FastPass can perform these operations even **from remote locations**. This is a service that the Service Desk is not able to provide to the user. The time savings and productivity gain for the user is significant.

## Multi-System Password Reset

Enterprises have different applications and systems with different password policies. Some organizations use Single Sign-On or Password Synchronisation to tackle this problem. Often it is not accepted to use the same password for systems with different levels of IT security impact or if you're not able to harmonize password policies.

Organizations like NIST for instance (FIPS PUB 199) recommends resources to be categorised as low impact, moderate impact or high impact, and the user should not share the same password between the different categories.

To respond to that FastPass Multi-System Password Reset is an option. From the admin console you configure this and the user can then reset passwords for each individual resource. If the user wishes to reset a password for Active Directory, he selects AD; and if he needs a different password for SAP, he just selects SAP or selects a specific SAP instance.

## Single Password through Password Synchronization

The number of systems, and therefore accounts and passwords that information workers need to access is increasing year by year. Much effort is devoted to combating this problem, but problem persists, so the time for solving this is up. The most cost-effective solution is to standardize passwords through Password Synchronization. FastPass delivers a strong, flexible approach with a wide range of connectors for different systems and applications. Synchronization is transparent, triggered by a normal password change and controlled by the user accessing FastPass Password Manager. The most used connectors are for SAP, iSeries (AS400), SQL and Oracle. FastPass also comes with a set of generic connectors that allows you to build connectors to your own solutions and thus making FastPass the one solution to handle password across the board for all of your applications and systems.



#### Hardware requirements for FastPass server

- 2800 MHz Pentium compatible CPU
- 1 GB RAM
- 1 GB hard disk space for log and audit

#### Software requirements for FastPass Server

- Microsoft Windows Server 2003 SP1 or later
- Microsoft Internet Information Server (IIS) v. 6.0 or later
- .Net Framework v. 2.0
- Microsoft ADAM SP1 or later (ADLDS)

#### Supported web browsers

- Microsoft Internet Explorer v. 6.0 or later
- Mozilla Firefox v. 2.0 or later

#### Supported clients & servers

- Windows XP SP2 or later
- Windows Vista
- Windows 7
- Windows Server 2003 R2 or later
- Windows Server 2008

#### Supported mobile browsers

- Windows mobile
- Blackberry
- Symbian OS
- iPhone

#### Connectors for Password Synchronization to

- Windows: AD/ADAM (ADLDS)
- iSeries (AS/400)
- SAP
- MS SQL
- Oracle
- UNIX
- Generic\*

\*API and sample code is available for building custom password connectors.

#### Languages supported

- English
- Spanish
- German
- French
- Dutch
- Danish
- Swedish
- Norwegian

## Enhance Security

The FastPass Password Manager allows organizations to implement more secure policies. Security is increased by:

1. making password changes a private issue
2. eliminating accidental user identification by Service Desk staff
3. reducing the need for users to write down passwords and
4. enabling the use of more complex passwords and a higher change frequency.

## Zero administration

FastPass administers and enrolls users automatically. Users are discovered by FastPass based on AD group membership and so addition and deletion of users happens when the changes are made to the AD groups. Users will automatically be invited to enroll in FastPass. You can set up that user will receive reminders by mail or SMS until they do enroll. Other features to secure user enrolment are available in FastPass – a NAG screen will appear on the monitor until they have enrolled. Furthermore, the Service Desk can force users to enroll if the user calls the Service Desk with a password problem. In this way, FastPass helps you take full benefit from your business, which relies on enrolled users!

## Help Desk client

Even with the most advanced end-user tools, some users will continue to call the Service Desk with questions regarding their passwords. They may have forgotten the answers to challenge questions, or they may have technical queries. With the Help Desk client, Service Desk analysts are able to provide fast, secure and efficient service to the end-user. One of the features is to allow Service Desk analysts to issue a PIN-code which allow the user to access and enroll in FastPass. This is considered the preferred route, as the user might call back again next month with a forgotten password request and also to sustain the secure process: "never give out a password over the phone".

## Leverage Your Existing Infrastructure

The FastPass Password Manager is a productivity add-on for your existing Windows Server environment. FastPass utilizes Active Directory as the user repository and ADAM (ADLDS) as data store. The solution will let you take further advantage of these infrastructure components and the investments you have already made. FastPass is prepared to forward user events into any Service Management system you are using. FastPass can be configured to achieve high availability and to meet the strongest of security demands. FastPass has a scalable architecture to serve even hundreds of thousands of users.

## Password Self-Service from Anywhere

In today's technology-driven environment, the ability for users to access information from any place, at any time, is essential. Users access a broad range of software applications from computer desktops or other platforms such as mobile phones. The FastPass Password Manager is available with different interfaces that allow the users to reset their passwords anytime and anywhere. Users can access FastPass from a variety of standard browsers and mobile devices and even from the login screen of your desktop operating system.

## Password Filter enables Policy Enforcement

Password policies play an important role in security, as users tend to select passwords that are simple and easy to remember. More mature operating systems, such as Windows Server, contain better features to ensure suitable complexity of passwords, but many applications do not. The Password Filter enables administrators to adjust policies to fit all the implemented systems and applications. This enables you to better comply with up-to-date security standards. Furthermore, Password Filter enables security administrators to define stronger and more granular policies than those available in Active Directory.

## About FastPassCorp

FastPassCorp is a global provider of self-service password reset solutions for Active Directory and beyond. FastPassCorp is headquartered in the greater Copenhagen area, Denmark. FastPassCorp A/S is listed on First North, NASDAQ OMX Copenhagen Stock Exchange [FASTPC]