

# The Essentials of Enterprise Password Management

FastPass Password Manager V 3.4  
Enterprise & Service Provider Editions



## OVERVIEW

When deciding on a new Password Management System, companies have asked us for advice on the most important criteria for choosing between different offerings and solution models.

Our experience is that it is important to focus on the functions which determine the value of the particular business case, and which define future flexibility.

We have selected the functions which are important to all organizations and especially to larger organizations with many applications and many users working from different locations. In this document we have added a short description of FastPass Enterprise features related to the different headings. If you're considering alternative solutions to FastPass, then these are the areas where you should compare the quality.

If you are looking for more information and inspiration, the National Institute of Standard and Technologies (NIST) have issued a draft document: Guide to Enterprise Password Management (Draft) Special Publication 800-118, where you can find recommendations regarding the use and management of Passwords.

We consider the following topics to be the most critical ones:

- User registration
- Catch-22: The PC is locked
- Different passwords for different applications and security levels
- Service Desk tools
- Strong authentication
- All users – anywhere
- Infrastructure and flexibility

## User registration

When you need to get thousands of users enrolled into your Password Solution, you begin to realize the importance of an automated ongoing process.

It is not just enough to send out an e-mail to all users. Based on our experience only between 5% and 20% of the users will take the time to register and enrol themselves into the system. The consequence is that possibly 80%-95% of your users will call the Service Desk. Alternatively, you may have to do a manual process, whereby your administrators need to remind users and their management to enrol. This could indeed compromise the business case for the entire project!

FastPass offers an automatic process covering the complete enrolment process. With the toolset provided you should aim for an enrolment percentage of not less than 90%. The critical components are:

- Automatic discovery of users
- Automatic invitation mail to new users
- Automatic and ongoing reminders, by mail or SMS(text) to users who have not yet enrolled
- Help Desk PIN-code can be issued to users calling the Help Desk without being enrolled. The users must then enrol before they can reset the password by themselves.
- NAG screen repeatedly alerting users who have not yet enrolled

You can define individual enrolment profiles for different user groups based on your knowledge of how you can get the fastest action!

## Catch-22: the PC is locked because of a forgotten password

When a user has forgotten the password to the PC he is not able to logon. The user then calls the Service Desk, who will reset the password in Active Directory. Users can then use the new password given by the Service Desk - provided they're on the domain!

If the user however is *outside the domain*, the Service Desk is not able to help him. The PC will remain unavailable until he's back in the office and attached to the domain.



FastPass Enterprise solves both situations. A very small program at the PC allows the PC, via a browser, to connect to the FastPass portal and change Password in the AD. The user can then log-in when he is on the domain. The same action happens when he is on a remote net. In this case FastPass opens a 'hidden' VPN connection, where the Password is synchronized back to the PC.

The business benefit for the user and the company can be substantial, as this feature means that the user can keep working in the remote environment. Without this solution in place a complete journey might be lost when a PC password is forgotten.

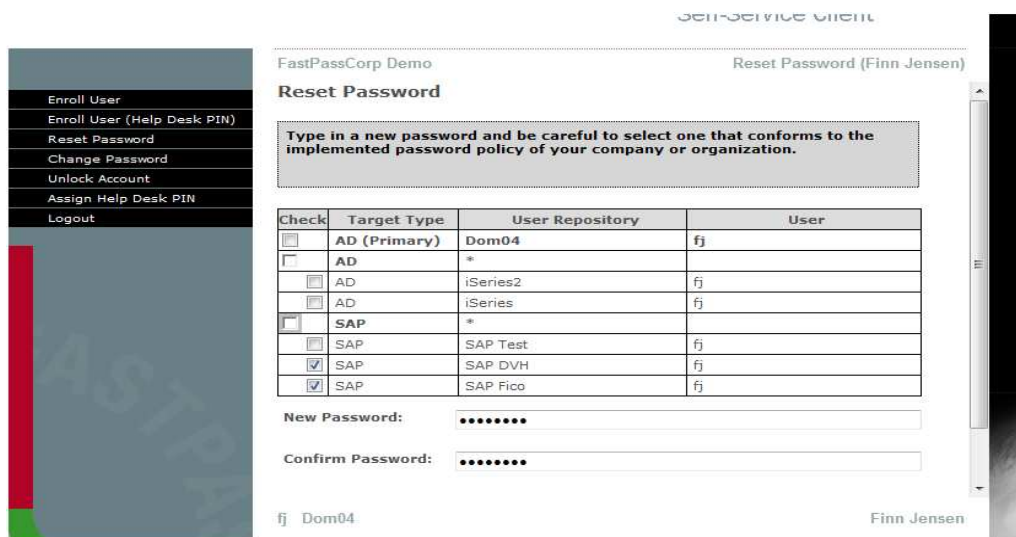
## Different passwords for different applications and security levels

Organizations like NIST for instance (FIPS PUB 199) recommend 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. In some organizations the single password concept - through password synchronization between applications with similar policies - is a good solution.

The consequence for Password Management in the situation with multiple passwords is that the user must be able to reset different passwords for different applications. When a user has the tool to reset forgotten passwords, then the cost of multiple passwords – due to high rate of resets - will be very limited. This makes it realistic to combine the demands from IT-security with the demands from the Service Desk when it comes to passwords and password resets.

FastPass Enterprise allows administrators to choose between password synchronization and selective password reset (reset on each individual system). FastPass provides advanced configuration tools to tie your multi system requirements to different user groups with different profiles.

As an example of that, if a company has Active Directory passwords and SAP passwords and wants different passwords due to different policies on those systems, then the user will simply select whichever system the password reset is targeted for.



Check	Target Type	User Repository	User
<input type="checkbox"/>	AD (Primary)	Dom04	fj
<input type="checkbox"/>	AD	*	
<input type="checkbox"/>	AD	iSeries2	fj
<input type="checkbox"/>	AD	iSeries	fj
<input type="checkbox"/>	SAP	*	
<input type="checkbox"/>	SAP	SAP Test	fj
<input checked="" type="checkbox"/>	SAP	SAP DVH	fj
<input checked="" type="checkbox"/>	SAP	SAP Fico	fj

If a user has different user-ids for the different applications, FastPass ties the different user-ids together and can synchronize and reset with multiple passwords.

For more information on differences between Single Sign-on and the FastPass solution, please visit our corporate web-site or contact FastPassCorp.

## Service Desk tools

No matter what enrolment rate you have achieved, you should still expect users calling in to the Service Desk for assistance. The Service Desk analyst needs to do user authentication before he can help the user with a forgotten password or a re-enrolment into FastPass. FastPass helps the Service Desk employee to verify the identity of the user.

In a Multi system environment and in synchronization environments, users call more when they meet technical difficulties in this more complex environment. The FastPass Help Desk Client provides specific information to support the Service Desk employee in performing his service to the user.

As a Service Desk manager, you prefer to have one central overview on service-level and workload for the Service Desk. This overview is obtained from the Service Management tool in place. FastPass is easily integrated into any Service Management tool and provides out-of-box integration to several solutions.



The net result for the Service Desk Manager is that all Password related calls which might slip past the Self-service Portal, will be handled quickly and efficiently, so that the business case for Password Management remains solid.

## Strong authentication

When a user wants to reset his password via Self-service, the password reset solution will authenticate the user as the first step. The authentication must correspond to the security level of the applications which the user can access. If the user has access to critical business systems, the authentication should be at least as strong as the authentication for the application.

FastPass allows the administrator to define different profiles for different groups of staff members, in order to provide both the required security level and also

provide user convenience. Authentication of users should not be stricter than necessary; hence the need for dynamic authentication profiles.

FastPass will combine three different methods for Self-service authentication:

- Your location (IP-address)
- Something you remember (Private challenge questions)
- Something you have (Mobile phone)

The administrator can define different profiles ranging from one method to all three methods for very secure users or critical applications. In FastPass the administrator configures profiles that *dynamically determine the authentication* of the user. If a user is on a secure net then it may be OK to authenticate with just challenge questions; but if the same user is on the external net, an authentication profile could be configured to demand both challenge questions and an SMS-pin code to securely authenticate the user.



For users with very high authentication requirements, you can even configure FastPass to require that a Help Desk PIN is used as part of the process of validating the user. In this way the Service Desk staff member can demand a personal presentation before issuing the PIN-code.

With regards to the challenge questions, you can decide what challenge questions, and how many, a user must answer correctly to be authenticated in different situations and/or locations.

## All users – anywhere

In today's business environment organizations have many different types of users and devices accessing systems and business applications from different locations. Most users have PCs owned by the domain; but there are external users (like external consultants) who have access to some resources on the IT-system. FastPass supports all users in the different situations.

The situation for a domain user is that a forgotten password means that he can't access the PC – in which case he uses the PC-client component of FastPass.

For an external user the PC password and the domain password are different, so he can access his PC locally, but he can't get on the company network.

The FastPass windows client will enable users to access FastPass remotely, even if he's outside the domain. If a domain-PC does not have the windows client installed, then the user can access FastPass through a browser on another device, from where he can reset the password.

With access to FastPass, via a link on the organization's intranet or extranet, the external consultant can get access to FastPass Self-service and reset the password on AD. Then he can immediately log-on to the network again.



A user might even reset the password from a mobile device (Smartphone, iPad etc.) using a mobile browser.

Overview:

FastPass Enterprise	Internal net	External net
Domain user	YES	YES
External user	YES	YES

## Infrastructure and flexibility

One of the most compelling features of FastPass is that it is in essence an *add-on to your existing Windows Server environment*. As a web-based self-service solution for users already in AD, this is part of your server environment utilizing user data, group memberships and policies already in place.

This means, from an *implementation point of view*, that it's really fast to implement. From an *operational point of view* this is also very important. You do not add yet another system to operate. With just a few hours of admin training, Windows Server professionals can be up to speed with FastPass.

Larger organizations may have complex environments with several domains and even a forest structure which is supported by FastPass Enterprise. But even smaller organizations may have a need for a multi-domain solution. If your company is buying another company, or has internal and external user groups, then you may have a need to support more domains. Also, if you're in the process of upgrading from Windows Server 2003 to 2008 then it can be very useful to let the users have two accounts for a period of time and have FastPass synchronize the passwords.

For Managed Service Providers, there is a need to be able to handle more organizations from the same console and system. So if you're an MSP this is definitely a must-have. Even if you're an organization which might consider outsourcing of your Windows Servers at some point in the future, you're in a good position to negotiate this contract with a tool in place which is built for MSP environments.

A *flexible browser based* solution will not only ease deployment of the solution, but also give you the opportunity to let password self-service become a feature on your intranet with the same look and feel and visual elements that your users are familiar with.

*Multi language* is important to many organizations working overseas. This will avoid end user training for the solution, and will also allow the end users to handle challenge questions in their native language, avoiding confusion for the users.