The essentials of password self-service for enterprises

The essentials of password self-service for enterprises

The essentials of password self-service for enterprises

OVERVIEW

When deciding on a new Password self-service solution, companies have asked us for advice on the most important criteria for choosing between different offerings and solution models. With this document we hope to help organizations in the early phases of a buying process.

Basically password self-service solutions are implemented to achieve the following:

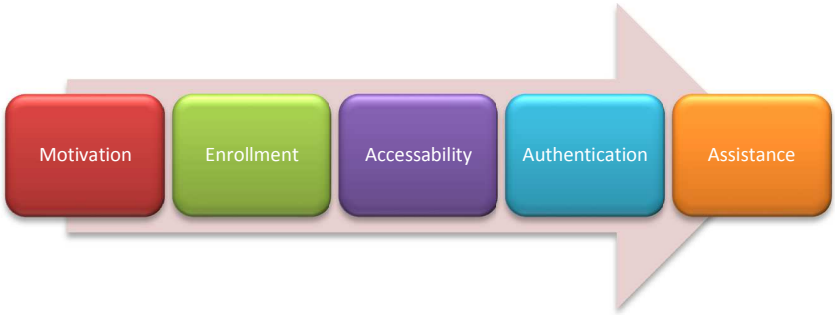
1. Reduce service desk workload as password calls disappear
2. Improve end-user service (faster process and 24/7)
3. Better password security and compliance

No matter what your reasons are, the key performance indicator (KPI) for a password self-service system must be **the percentage self-service calls compared to total calls related to passwords.** We have seen examples of no more than 20% and examples of more than 90%.

To reach 90% or more focus must be on the processes and use-cases. To have efficient processes depend however on the product you use – it is most often interconnected.

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.

Password self-service success depends on 5 steps which we have identified together with our customers:



1. Motivation step

The purpose of the motivation step is to help users understand the reason for new service. It is important to inform users in advance of the changes coming and why the company invests in new processes.

The essentials of password self-service for enterprises

An important aspect is to be honest about the expected results for the company: Higher productivity and improves security related to passwords. This is why the new service is introduced.
It is up to every organization to prepare users in accordance with normal communication policies for company news.

For companies with **multiple passwords** we have met an important pitfall. From a technical point of view implementation might only be for the most popular password like Windows/AD. If the user however has other passwords like SAP passwords, there is a high risk that the user motivation decreases, as he might think, that it is the SAP password he forgets – so why bother with the new system! Furthermore when a user is in a forgotten password situation he might not remember what password is in self-service, and then he might just as well call the service desk right away!

Our recommendation is to start the project **with passwords that cover more than 90%** of the password reset calls to the service desk.

Different passwords for different applications and security levels

Organizations like the National Institute for Standard and Technology (see FIPS PUB 199) recommend data resources to be categorised as low impact, moderate impact or high impact, and the user should not have identical password between the different categories. This means that there are situations where single sign-on and password synchronization can't be used.

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.

The essentials of password self-service for enterprises

FastPass Enterprise allows administrators to choose between password synchronization and selective password reset (reset on each individual system).

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.

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, and then he access the company self-service portal, where password self-service ia a component.

Overview of password self-service:

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

2. Enrolment step

In practically all variations of password self-service we need some information from the users to be used when they need to reset or un-lock the password. It can be answers to standard questions, a mobile phone number, private e-mails or other information.

Experience shows us that it is not enough to ask a user politely to enrol. We have customer examples varying from 6-35% as success of the first e-mail invitation send out! It is obvious that we cannot get a higher result of self-service than the enrolled percentages! This means that we need to get to 100% enrolled. If is entirely up to the IT department to run the process, you will get a high overhead of monitoring and resending reminders to those who failed the first time. In addition to this process the IT-department will have to remember to invite new users. This will not work in reality.

We suggest that you combine two processes:

3. A soft mailing invitation with motivation to enrol. The invitation can then be followed be a number of reminders where we get tougher. Depending on company culture this can get a high portion enrolled in a soft and acceptable way
4. A forced enrolment where the user's PC basically tells the user to enrol or he will not be able to use his PC until he has done so! The forced enrolment can be activated after the mailing process or can even be the only process.

Both strategies must be completely automatic to be efficient, and to avoid the overhead of management in the service desk.

In few situations and organizations you can consider if it is possible to avoid the enrolment process. If you only want to use SMS-pin codes and you already have control of the users' mobile-numbers you don't need to do so.
Some companies have user groups with access to un-sensitive data, and in these situations question/answers like what is your employee number can be uploaded, and the users don't have to enrol.

FastPass offers an automatic process covering the complete enrolment process. With this automatic 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.
- Forced enrolment via NAG screen enforcing the 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!

3. Accessibility to the password self-service

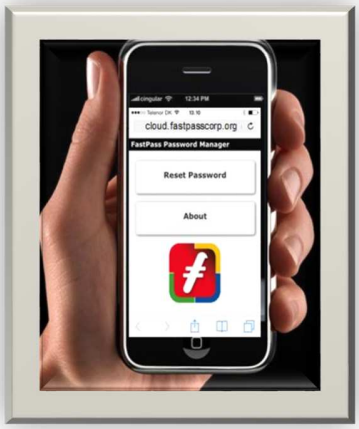
The most fundamental difference to other types of self-service is the fact that **the PC will normally be locked** when you have forgotten your password (Windows passwords). All considerations regarding access must solve this issue.

Modern users might have a company paid smartphone where you can get access to the internet and then to the self-service portal and do a password reset. *But what about the other users*? Can we ask them to go to a colleague and get WEB access on their PC? Then we interrupt their work (and might as well call the service desk) and there might not be a colleague around.

The essentials of password self-service for enterprises

The only acceptable solution is to use the user's PC for password self-service. This means that **the self-service solution must include a PC-client** allowing the user to use his otherwise locked PC!!

As many users expect to do self-service from their smart-phone or tablets it must be easy to do the password reset from the Smart-phone. Not instead of the PC but as an addition to reflect where the user might look for self-service!



Users on external network

Companies with travelling employees or many working from home have a serious password problem today. When a user forgets his Windows password the service desk can't reset the password in the PC-cache! This means that a forgotten password renders the PC useless, until it returns to the domain, where password synchronization between AD and PC takes place. The consequence for a user can be a wasted trip, and indeed many hours downtime.

The essentials of password self-service for enterprises

If this is a real challenge **it is essential to have support for remote PCs where the user in a secure way can reset AD and PC-cache password.** FastPass offers this through an advanced use of VPNs installed at the PC.

A technical reality of today is that in many situations it is not possible to get an internet cable; but access will only be through Wi-Fi hotspot. FastPass offers access through well-known or new Wi-Fi. Hotspots with browser-based security key input, is however not secure. For these situations we recommend that the user's smartphone is used as the hotspot!

4. User authentication

Authentication is the process of linking a user-id to a real person. We use the password for authentication. When the password is forgotten or locked we need to authenticate the user alternatively.

In many years the preferred method has been personal questions and answers based on a selection from a standard list of questions. This is an accepted way of authentication, experience shows however that some users (sometimes many users!) forget the answers or forget how they have spelled it. If the user can't answer the questions correct, he must call the service desk, and the self-service has no value.

This has led to a search for other authentication methods. The most popular being:

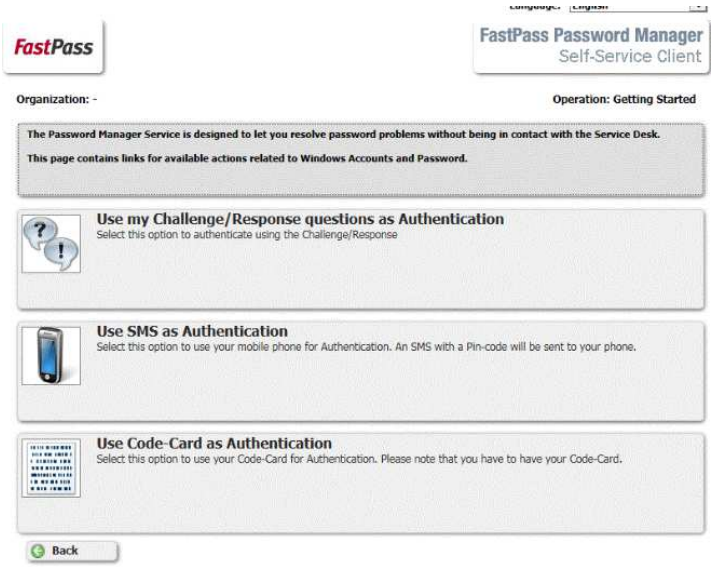
- SMS-codes to mobile phone numbers
- Use of private e-mails
- Use of individual questions
- Use of other physical tokens than the mobile phone
- Use of personal identification like fingerprint, iris scanning and voice.

All authentication methods have pros and cons. The pro of questions/answers is that it carries no cost and requires no special technology. This means that it will continue to be a popular authentication method – but some users can't remember!

We see the solution for the alternative authentication to be **to give the user free choice.** This means that when the user is asked to authenticate the self-service tool asks the user how he wants to authenticate. If the user has a token with him like his mobile phone, this will be the

natural choice. If the user however doesn't have a mobile phone or it is not available, ha can choose another method.

The very important consideration is, that it is not up to administration to decide for the user initially – but to let the user decide, when he is exactly in the situation.



Experience shows that it is easier for users to remember the answers to questions they have made themselves. This means that the question/answer authentication must have the possibility to **let users define their own questions** in addition to standard questions.

Strong authentication (2-factor authentication)

Where users have access to very sensitive information it might be a requirement that access demands strong authentication. General access from external net will often require 2-factor authentication. If this is the case with standard log-in then the process for user password self-service can of course not be weaker.

This means that it is an absolute requirement that the password self-service solution can be configured to demand 2-factor authentication always for some users and for all users under some circumstances – like coming from the external net.

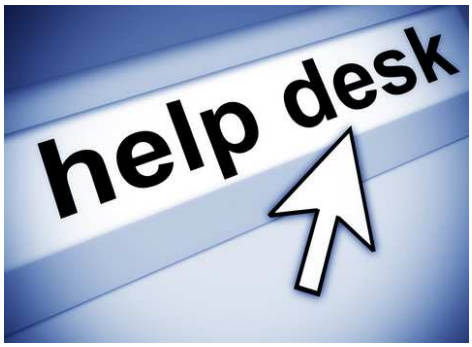
FastPass support 2-factor authentication where you combine something you remember with something you have (a token).

5. Assistance from the service desk

The essentials of password self-service for enterprises

No matter what enrolment rate you have achieved, you should still expect some 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 through information being presented from Active Directory and even by presenting some of the personal answers! (Answers can be configured to be semi-private where they are visible for the service desk, or as private where no one can see them)

If we give the user the password he is asking for, we know for certain that he will call the service desk again next time he forgets the password. The result of this process is the gradual deterioration of the business case. This is why **the service desk only gives the user a pin-code to reenrol in FastPass**. Then the user can immediately afterwards reset the password himself.



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.