

Passwords in Single Sign-On concept versus FastPass Enterprise Password Manager

Finn Jensen, CEO FastPassCorp, Jan. 2011

In the pursuit of faster and easier user access to IT resources in complex environments, many organisations are looking for technologies that can ease the login process for users. A popular technology is Single Sign-On (SSO), which requires the user only to log in once and then grants him access to all resources. An alternative to this technology is Password Synchronisation (also known as Simple Sign-On), which still requires the user to log into each individual resource, but uses the same password for all resources. The two models have a number of advantages but share a disadvantage with regard to security. FastPass Enterprise attempts to maintain the advantages whilst also solving the security issue. This document is inspired by the NIST draft document, 'Guide to Password Management (SP 800-118)'.

This document consists of two parts:

1. Quotations from 'Guide to Password Management (SP 800-118)' to present a general overview of the difference between SSO and Password Synchronisation (in blue text)
2. Description of some features of FastPass Enterprise Password Manager, which defines a new standard and new opportunities for Multi-Password environments

1. Guide to Password Management (NIST SP 800-118 draft):

A password synchronization solution takes a password from a user and changes the passwords on other resources to be the same as that password. The user then authenticates directly to each resource using that password; there is no centralized directory or authentication server performing authentication on behalf of the resources. The primary benefit of password synchronization is that it reduces the number of passwords that users need to remember; this may permit users to select stronger passwords and remember them more easily

Password synchronization solutions are typically easier and less expensive to implement than SSO technologies, but password synchronization also has significant security disadvantages. Because password synchronization causes the same password to be used for many resources, each of which stores the password or a hash of the password, the compromise of any one instance of the password compromises them all. This is particularly damaging if password synchronization is used for resources with significantly different security requirements—for example, a password on a low-security resource may be compromised relatively easily and then reused on a high-security resource that shares the synchronization solution. This allows an attacker to compromise a low-security resource to gain access to a high-security resource.

	SSO and RSO	Password Synchronization
Is the number of passwords that users have to memorize reduced?	Yes	Yes
Can the user authenticate without performing additional steps?	Yes	Yes
Is the number of authentications that users have to perform reduced?	Yes	No
Is the user largely unaffected if the password management technology is temporarily unavailable?	No	Yes
Is the impact of a user password for an individual resource being compromised limited to just that resource?	Yes	No

Organizations should also consider the impact level associated with the passwords that would be stored in a password management technology. If a technology is being deployed to support low-impact passwords, and the technology’s safeguards have been designed for that level, then it is generally unwise to use the technology for storing higher-impact passwords without reevaluating the strength of its safeguards. In some cases, it is appropriate to deploy a separate password management technology implementation for higher-impact passwords. This is particularly important for password synchronization solutions, which use the same password for each resource. If the resources are of varying security levels, such as both low and moderate-impact systems, an attacker could gain access to a user’s password by compromising a low-impact system, which is likely to be less strongly secured than a moderate-impact system. Because the user’s password is synchronized across resources, including moderate-impact systems, the attacker could then use this password acquired from a low-impact system to gain access to a moderate-impact systems. Organizations should take care to ensure that attackers cannot gain access to higher-impact systems by taking advantage of password synchronization across systems of varying impacts.

2. FastPass Enterprise

The major issue with SSO and Password Synchronisation is that one password allows a user to gain access to all resources. According to FIPS 199, organisations have to categorise all IT resources according to their IT security demands: low impact, moderate impact and high impact. You need different protection for the three IT security impact groups, and should also have different passwords. A password for a low-impact system might be stolen relatively easily, and should not be the key for a high-impact system.

To solve this problem, FastPass has extended FastPass Enterprise to cover this situation.

Applications and systems with the same security impact can share a password. FastPass allows synchronisation from Active Directory to other target systems. For systems with different security impact levels, the user can change and reset the password in FastPass for systems in the same category. The IT Security Officer might, for example, decide that all SAP operational systems must share the same password, but not be synchronised with Active Directory. These SAP instances can be grouped together in FastPass, and the user can simultaneously reset the password for the group.

In this way, the company can combine password synchronisation with differentiated passwords for different security impact groups.

It is worth remembering that the productivity gains delivered by FastPass, in terms of end-user self-service concerning forgotten passwords, will easily and quickly recoup the whole cost of investment.

The above NIST table can thus be modified to cover the extended needs and FastPass Enterprise:

	SSO	Password Synchronisation	FastPass Enterprise
Is the number of passwords that users have to memorise reduced?	Yes	Yes	Yes
Can the user authenticate without performing additional steps?	Yes	Yes	Yes
Is the number of authentications that users have to perform reduced?	Yes	No	No
Is the user largely unaffected if the password management technology is temporarily unavailable?	No	Yes	Yes
Is the impact of a user password for an individual resource being compromised limited to just that resource?	Yes	No	N/A
Different user passwords for different impact group systems (low, moderate, high)	No	No	Yes
Different authentication methods for resetting passwords for different impact group systems (low, moderate, high)	No	No	Yes
Different user passwords for applications with different password strength requirements	No	No	Yes
Cost to implement	High	Low	Low
Cost to operate	Medium	Low	Low

