FastPassCorp
PASSWORD SECURITY MADE EASY

FastPass Password Manager

Version 3.4.2

Microsoft AD integration notes

Document Title	Microsoft AD integration notes
Document Classification	Public
Document Revision	D
Document Status	Final
Document Date	April 23, 2012

Lyngby Hovedgade 98, 2800 Kongens Lyngby, Denmark.
http://www.fastpasscorp.com/

Limited Warranty
No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to documentation@fastpasscorp.com.

Table of Contents

1. Introduction

The document has been written April 23, 2012 and is targeted the FastPass Password Manager Version 3.4.2

1.1 Purpose

The purpose of this document is to describe the integration/interaction between FastPass Password Manager and Microsoft Active Directory (AD).

1.2 Audience

The intended audience of this document is personnel responsible for administration of the solution.

1.3 References

This document refers to the following documents:

None.

1.4 How to use this document

This document has a very limited scope and is expected to be read all in complete.

1.5 Terms

The following technical and product specific terms are used without further explanation throughout the document.

2. About FastPass Password Manager

FastPass Password Manager is a secure web-based solution offering self-service password operations to end-users.

Users are required to remember many more complex passwords on more systems than ever before. Research suggests that 30% of all calls to Help Desks are related to forgotten passwords.

Built to use Active Directory as the authoritative repository, FastPass are capable of delivering an instant ROI by deploying in just a few hours on your existing Microsoft environment. Further value can be gained by integrating these tools with Microsoft Identity Integration Server (MIIS/ILM 2007) for an industry leading Identity and Access solution.

Introduce Self-Service
Users only need a web browser to access FastPass whether on the corporate intranet or across the internet. In addition an easily integrated deployment via SharePoint Portal or the SAP Portal gives a secure single point of entry to all applications and supports anonymous access for users who have forgotten their passwords.

FastPass enables self-service enrollment and password resets as well as self service account mapping utilizing the same Web UI and saving directly into Active Directory. Captured password resets can be synchronized across multiple platforms without integration to Microsoft Identity Integration Server (MIIS/ILM 2007).

FastPass help to reduce the workload within the Help Desk, Increase end-user productivity and Strengthen Security
A Password Management solution from FastPassCorp saves both time and money for all parties involved: .

For Executives:

- Reduce workload in help desk
- Make it possible for your employees to access systems even when the Help Desk is closed
- Enhance security
- Leverage past investments in Active Directory or ADAM
- Achieve ROI within 3-9 months (no investment needed)

For Help Desk Managers:

- Remove 30% of calls to help desk
- Enhance logging and reporting
- Significantly lower total cost per forgotten password
- Increase employee satisfaction
- Easy implementation (from minutes to days depending on complexity)
- Easy roll-out using automated enrollment services

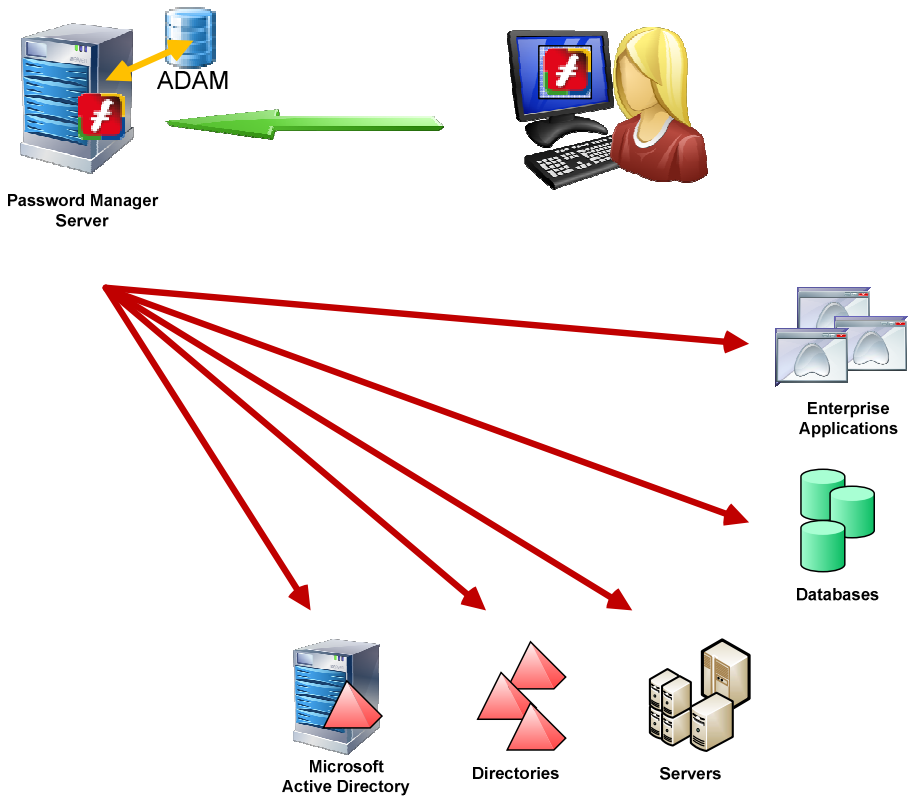
For Employees:

- Extremely fast solution to a forgotten password situation
- Access to systems 24/7/365
- No need to involve others
- No barrier to comply with strict password security policies
- Simple to use

2.1 The architecture of FastPass Password Manager

The following describes and illustrates the architecture of FastPass Password Manager.

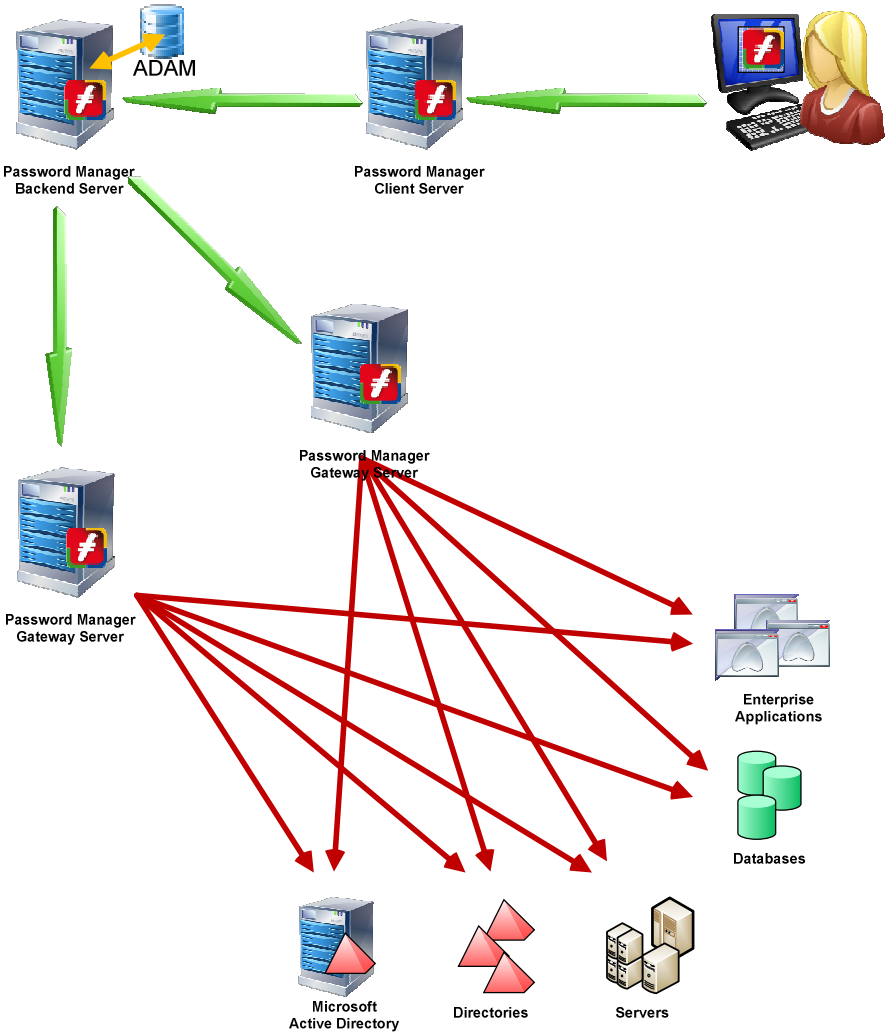
From a user perspective the Password Manager is offering web based self-service features to maintain passwords in the enterprise. This is what is illustrated below.



Logically the Password Manager Server is built of multiple sub components each offering its own set of functions for the total solution. The main components are listed in the table below:

Component	Description
Backend Server	Implement the control of all end-user transactions, communication to the Gateway Server, scheduled discovery of users in the domain infrastructure, control and coordination of password synchronizations, invitations of users and much more.
Client Server	Implements the Web-interface for the end-users and communicates with the Backend Server.
Gateway Server	Implements the access to the domain infrastructure and other Password Sync target systems.

All three main components are by default installed on the Password Manager Server and are directly configured to operate together. A full implementation can be built on additional Client Servers and Gateway Servers and this is shown on the illustration below.



The solution is built as a service oriented architecture meaning that all main components are web services implemented in Microsoft Internet Information Server (IIS) and communication using SOAP over HTTPS.

2.2 Integration to Microsoft Active Directory

Password Manager supports easy integration into multiple Microsoft Active Directories from a single implementation. The configuration is done from the Password Manager Administration Client implemented as part of the Password Manager Backend Server. The communication to the Active Directory infrastructure is done from the Password Manager Gateway Server. The integration is implemented using LDAP v3 communication and this can optionally be implemented to use either secure mode or SSL mode. Secure mode is the default and the one used by Microsoft Active Directory internally for synchronizing passwords between Domain Controllers.

Password Manager requires the following parameters to be configured to be able to access a Microsoft Active Directory Domain.

Parameter	Description
Domain Name	The full qualified domain name of the domain like mycorporation.com.
Domain Alias	A label typically the same as the NetBIOS name for the domain which is what is

	shown in desktop login interfaces.
LDAP Base DN	The distinguished name (DN) to use as the offset in the LDAP tree structure. This can point to an Organization Unit (OU) like in OU=Employess,DC=mycorporation,DC=com or to the root node like in DC=mycorporation,DC=com.
Connection Mode	The connection mode to use for the communication. Microsoft Active Directory offers the modes normal, secure and SSL but Password Manager only supports Secure and SSL mode. The secure mode used Kerberos for the authentication which is dependent on normal domain communication from the Password Manager Gateway Server and to the Domain Controller in addition to communication on port 389 (TCP). The SSL mode requires a certificate to be implemented on the Domain Controller which is not a trivial task but then as an advantage it only requires communication on port 636 (TCP) from the Password Manager Gateway Server and to the Domain Controller.
Domain Account Name	The name for the account with privileges to read user attributes and to reset passwords.
Domain Account Password	The password for the account specified.

In order to support a higher fault tolerance Password Manager can be configured to access multiple domain controllers in the same domain possibly with an offset from different Password Manager Gateway Servers. To configure in this way the following information must be configured for each connection to the Domain.

Parameter	**Description**
Domain Controller	The fully qualified hostname or IP address for a domain controller. If SSL mode is desired for the communication then the fully qualified hostname is required.
Gateway Server	The Password Manager Gateway to use as offset for the specified Domain Controller.

All parameters are stored in the Password Manager Data Storage (ADAM) and sensitive information like account name and password is stored with strong encryption.

The next section describes in details the LDAP operations that are performed against Microsoft Active Directory and the needed privileges for the Domain Account to be functional.

3. Function details for Password Manager AD integration

The following describes in details the LDAP operations that are performed against Microsoft Active Directory and the needed privileges for the Domain Account to be functional.

The Password Manager integration is using the following functions/methods against Microsoft Active Directory:

- Discover Account
- Reset Password
- Change Password
- Unlock Account
- Discover Groups

These functions are described below.

3.1 Details for the Discover Account function

The Discover Account function is performed as part of any end-user transaction in Password Manager to keep the Password Manager Data Repository (in ADAM) updated. The data marked as "Stored" in the tables below are data on the user accounts that will be stored in FastPass.

Required permissions

The Discover Account function requires read permissions granted to the Domain Account on a number of attributes that are then stored in the Password Manager Data Repository for each user. By default the attributes shown in the following table is used.

Attribute	Access	Description	Stored
DistinguishedName	Read	The unique name in LDAP format for the user.	Yes
sAMAccountName	Read	The short unique name for the user (the old style login name).	Yes
objectClass	Read	The AD object	Yes
cn	Read	Common Name for the user.	Yes
sn	Read	Sur Name also editable in Active Directory Users and Computers.	Yes
givenName	Read	First Name also editable in Active Directory Users and Computers.	Yes
displayName	Read	Full Name also editable in Active Directory Users and Computers.	Yes
description	Read	Description also editable in Active Directory Users and Computers.	Yes
department	Read	Department also editable in Active Directory Users and Computers.	Yes
title	Read	Title also editable in Active Directory Users and Computers.	Yes
manager	Read	Manager also editable in Active Directory Users and Computers.	Yes
phone	Read	Phone also editable in Active Directory Users and Computers.	Yes
mobile	Read	Mobile Phone also editable in Active Directory Users and Computers.	Yes
mail	Read	E-mail address also editable in Active Directory Users and	Yes

		Computers.	
lockouttime	Read	Used to determine whether a user has been locked because of too many failed login attempts.	Yes
userAccountControl	Read	Used to determine whether a user has been disabled.	Yes
memberOf	Read	The Groups a user is member of.	Yes
primarygroupid	Read	Used to determine the primary Group of a user.	Yes
userPrincipalName	Read	The user principal name of the user	Yes
pwdLastSet	Read	Used to determine whether a user has been locked because of too many failed login attempts.	Yes

The list of attributes can be extended by customization and if this is performed then Read permission for these attributes must also be granted.

3.2 Details for the Reset Password function

The Reset Password function is performed as part of the Reset Password end-user transaction in Password Manager to perform the actual reset of the password but only if the user has passed the configured alternative authentication methods and only if the user holds the “Change Password” privilege.

By default the Password Reset function first performs a password reset operation to a random generated password and then performs a password change operation **to the by the** user specified password. This flow is needed to ensure that the policy checking against the password history is performed. A consequence of this flow is that the password history count is incremented on each operation.

Required permissions

The Reset Password function requires read permissions granted to the Domain Account on a number of attributes but that are all listed in the table for Discover Account. Further it requires permissions granted to the Domain Account on the attributes shown in the following table.

Attribute	Access	Description	Stored
lockouttime	Write	Used to determine whether a user has been locked because of too many failed login attempts.	Yes
pwdLastSet	Read-Write	When the user last set the password.	Yes
userAccountControl	Read-Write	Used to determine whether a user has been disabled.	No
msDS-User-Account-Control-Computed	Read	Used to find out the LOCKOUT setting	No
ntSecurityDescriptor	Read		No
logonHours	Read	Used to get user’s valid logon hours	Yes

Besides the listed attribute rights the function also requires the privileges listed in the following table granted to the Domain Account.

Privilege	Access	Description
ResetPassword	Execute	Method used to set the password.

Besides the listed attribute rights and privileges the Reset Password function also requires the privileges listed in the following table to be granted to the Domain Account on the Domain Policy object.

Attribute	Access	Description	Stored
maxPwdAge	Read		No
minPwdAge	Read		No
minPwdLength	Read		No
lockoutDuration	Read		No
lockOutObservationWindow	Read		No
lockoutThreshold	Read		No
pwdProperties	Read		No
pwdHistoryLength	Read		No
objectClass	Read		No

3.3 Details for the Change Password function

The Change Password function is performed as part of the Change Password end-user transaction in Password Manager to perform the actual change of the password but only if the user has passed the configured alternative authentication methods and only if the user holds the "Change Password" privilege.

Required permissions

The Change Password function requires read permissions granted to the Domain Account on a number of attributes which are all listed in the table for Discover Account and no other privileges are required.

Attribute	Access	Description	Stored
userAccountControl	Read-Write	Used to determine whether a user has been disabled.	Yes
pwdLastSet	Read	When the user last set the password.	Yes
msDS-User-Account-Control-Computed	Read	Used to find out the LOCKOUT setting	No
ntSecurityDescriptor	Read		No
logonHours	Read	User's valid logon hours	Yes

Besides the listed attribute rights the Change Password function also requires the privileges listed in the following table to be granted to the Domain Account on the Domain Policy object.

Attribute	Access	Description	Stored
maxPwdAge	Read		No
minPwdAge	Read		No
minPwdLength	Read		No
lockoutDuration	Read		No
lockOutObservationWindow	Read		No
lockoutThreshold	Read		No
pwdProperties	Read		No
pwdHistoryLength	Read		No
objectClass	Read		No

3.4 Details for the Unlock Account function

The Unlock Account function is performed as part of the Unlock Account end-user transaction in Password Manager to perform the actual unlock of the account but only if the user has passed the configured alternative authentication method.

Required permissions

The Unlock Account function requires read permissions for the Domain Account to a number of attributes which are all listed in the table for Discover Account. Further it requires the following permissions to the attributes shown in the following table.

Attribute	Access	Description	Stored
Lockouttime	Write	Used to determine whether a user has been locked because of too many failed login attempts.	Yes
pwdLastSet	Read	When the user last set the password.	Yes

3.5 Details for the Discover Groups function

The Discover Groups function is performed as part of the Security Settings for a domain in the Password Manager Administration Client to collect the available groups from Microsoft Active Directory.

Required permissions

The Discover Groups function requires read permissions granted to the Domain Account on a number of attributes which are all listed in the table for Discover Account. Further it requires the following permissions granted to the Domain Account on the attributes on the Group objects.

Attribute	Access	Description
name	Read	The name of the group
distinguishedname	Read	The unique name in LDAP format for the group.