

Migrating application users and passwords with Password Manager



Contents

1	Introduction	1
2	Migrating Users	1
3	Initializing Passwords	2
4	Maintaining Passwords During the Transition	2
	APPENDICES	3
A	LDIF Example File	4
B	SQL Example File	5

1 Introduction

This document describes a number of ways in which Hitachi ID Password Manager can be used to ease system and directory migrations.

Examples of migrations include, but are not limited to:

1. Upgrading a Novell NetWare / eDirectory environment to Windows 2008 / Active Directory.
2. Moving from one mail system (e.g., Lotus Notes) to another (e.g., Microsoft Exchange).
3. Replacing one LDAP directory product with another.
4. Rolling out a new application that impacts a large user population, such as a self-service human resources (HR) portal.

As will be described below, Password Manager can assist in the initial activation of the new system or directory and in the transition period where both the old and new systems are active.

2 Migrating Users

As a part of its nightly automation process, Hitachi ID Password Manager extracts a list of users from every system where it manages passwords.

When migrating users to a new directory, these user lists are a natural place to start to get a list of users that should be created on the new system.

For example, the following command can be used to extract a list of user IDs and full names from the Password Manager database:

```
c:  
cd "\Program Files\P-Synch\..\util\dumpdb user -trim -delimited > c:\temp\users.txt
```

This list of users can be manipulated into SQL commands to create database users or an LDIF file to create LDAP or AD users. Details of the LDIF or SQL files vary, but ?? on Page ?? and ?? on Page ?? include some examples:

Another key advantage of using Password Manager in an application or directory migration project is the ability to create new login IDs with random initial password values and avoid distributing password values by e-mail.

3 Initializing Passwords

A major problem in activating a new system is selecting a suitable initial password for users, and communicating that initial value to users securely.

Setting the initial password value to a user's SSN or login ID is insecure. Setting a stronger password is better, but communicating that initial value to users by e-mail is also insecure.

With Hitachi ID Password Manager, users need not know the initial password value to their new account. Instead, they can be instructed by e-mail to change all of their passwords, including the new one, with Password Manager. This way, they change their password from an initial random string (which they do not know) to a strong value securely, after proper authentication (with another system's password).

For example, new users of an LDAP directory might receive an e-mail with the text:

Acme, Inc. has activated a new corporate directory. New applications, and our Intranet, will verify your identity using a user ID and password on this directory.

To activate your corporate directory account, click on the link below, enter your windows network login ID and password, and select a new password for all of your accounts. You will then be able to use the new password both for the systems with which you are already familiar, and for the new corporate directory.

<http://password.acme.com/psynch/nph-psf.exe>

Users would follow the link, type their existing Windows NT login ID and password, and select a new password. They will then be able to log into every system, including the new LDAP directory, with the new password. Thus migrating users can be done efficiently and securely.

4 Maintaining Passwords During the Transition

In the event of a directory migration (for example, upgrading a domain from NetWare NDS to Windows 2008 Active Directory), it may be useful to keep running both systems for a transition period.

In these cases, the password synchronization features of Hitachi ID Password Manager will significantly reduce the complexity for end users, as they won't really have to understand which resources use which directory (and hence which password).

This will directly reduce the support load produced by the transition period.

APPENDICES

A LDIF Example File

```
dn: CN=FRIT0000,CN=Corporate,DC=ad-idslite,DC=hitachi-id,DC=com
changetype: add
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: user
cn: FRIT0000
description: Randell Fritz
distinguishedName: CN=FRIT0000,CN=Corporate,DC=ad-idslite,DC=hitachi-id,DC=com
userPrincipalName: randell.fritzad-idslite.hitachi-id.com
mail: randell.fritzad-idslite.hitachi-id.com
givenname: Randell
sn: Fritz
displayName: Fritz, Randell
telephoneNumber: (972) 116-3406
homePhone: (972) 116-3406
streetAddress: 822 Seventh Ave.
l: Dallas
st: Texas
c: US
postalCode: 44820
name: FRIT0000
userAccountControl: 514
sAMAccountName: FRIT0000
```

B SQL Example File

```
insert into hrapp.person
  ( employeeNum, loginID, firstName, lastName, streetAddress,
    city, state, zipCode, homePhone, emailAddress, startDate,
    status )
values
  ( "E000001", "HOPK0000", "Wilber", "Hopkins", "123 Second St.", "San Antonio",
    "Texas", "48840", "(830) 941-6880", "wilber.hopkinsad-idslite.hitachi-id.com", "1996-09-01",
    "ACTIVE" );

insert into hrapp.pii
  ( employeeNum, dateOfBirth, socialSecurityNumber,
    driversLicenseNumber, mothersMaidenName )
values
  ( "E000001", "1974-01-24", "262-46-5300", "823758-636", "Harris" );
```