

White Paper: Using Lieberman Software Corporation's Server to Server Password Synchronizer

Rev 2 – June 1, 2006

Lieberman Software Corporation
<http://www.liebsoft.com>

Abstract

This paper offers step-by-step instructions for using Lieberman Software's Server to Server Password Synchronizer.

Contents

1. Introduction	3
2. How Password Synchronizer Works	4
3. Setting Up Domains for Synchronization	5
4. The Internal Database	6
5. Time Skews	7

1. Introduction - Theory behind the passwords themselves

LAN Server and NT both store passwords in a form of representation known as a hash. A hash is the mathematical result of taking a password and putting it through a non-reversible function that generates a numeric value. In the case of LAN Server and NT, the hash values for any length password (passwords are limited to 14 characters in length) are 16 bytes. There are two possible hash functions used: DES hash and MD4 hash.

Example of a DES hash from LAN Server:

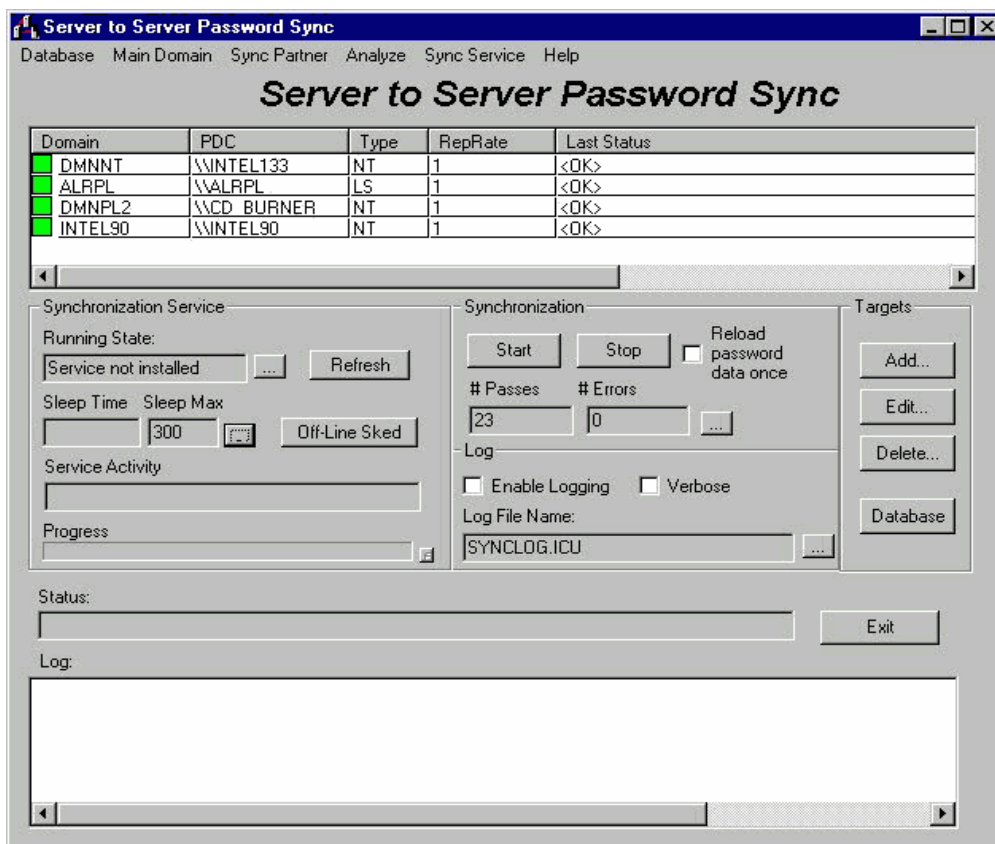
```
Password_Encrypted=FB842CFC6FCE70F9AAD3B435B51404EE
```

When you create a new password in NT, both the DES and MD4 hashes of the password are stored within the user account database known as the SAM. In LAN Server a DES hash is created for each user account. Fortunately for both you and I, the DES hash used in LAN Server and NT produce the same hash for an identical password. Consequently, a hash from LAN Server's account database can be placed into an NT server SAM and can be used to authenticate the user. And, a DES hash from NT can be imported into a LAN Server account database (NET.ACC) to allow a user to use the identical password in both LAN Server and NT.

2. How Password Synchronizer Works

The password synchronizer runs on an NT 4.0 machine (workstation or server) and maintains a database of users, their passwords, and the time and date of their last password change. This program periodically goes to every domain (both LAN Server and NT) and queries the user accounting system for any time stamp changes on user passwords (the time stamp changes when a password is changed). If a new time stamp is found, the new password hash is imported into the local database and checked against the database of locally stored passwords for other domains. If there is a new time stamp and new password, this new password will be pushed into the other domains.

The main screen of the program allows you to force synchronization at any time, as well as to add/remove/edit domains that will participate in the synchronization:



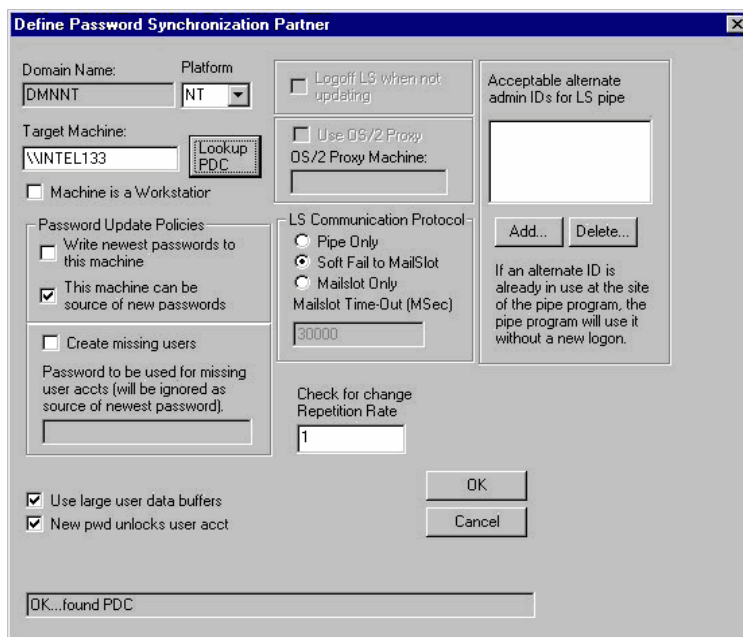
The most fundamental question is to decide which users are to be synchronized and on which domains. You must select a single domain that will contain the master list of all possible users to be synchronized. This is the Main Password Domain. Since you probably don't want to synchronize all possible users, we use a global group of your choice (on the main domain) to act as a source of users to synchronize to all participating domains. The group of users to be synchronized everywhere is known as All Domains Sync Group.

Since you don't want to use all of your network bandwidth checking for passwords, you can set a Sync Delay that will cause the password synchronizer to sleep between account timestamp checks. Since some domains experience more change than others, you can also set the repetition rate for synchronization to allow you to check one out of every "n" times for changes in the password in each domains.

3. Setting up Domains for Synchronization

In NT, there is no need to load any special software on the clients or servers in the domain. For LAN Server domains, we have a special agent program that you must start on the domain controller of the LAN Server domain. It is important that you establish administrator accounts that have fixed passwords that exist on the master NT domain as well as the target domains.

Here is a screen shot from the domain editing screen:



4. The Internal Database

The synchronization process depends on the local database maintained on the machine that is running the password synchronizer. To see the internal database in different views, you select the detail view:

Show password account details

User	Domain	DES Hash	MD4 Hash	Time	Time32	ExpDate32	ExpDate...
A	DMNNT	078E9B46...	3739F5F75...	Mon Dec 2...	349e2c22	ffffff	Unknown
A	DMNPL1	1C3A2B6D...	000000000...	Tue Dec 1...	3497794c	ffffff	Unknown
A	DMNPL2	1C3A2B6D...	C4DB8397...	Sat Dec 13...	34933fa2	ffffff	Unknown
AAA	DMNNT	000000000...	50E649944...	Thu Dec 1...	3499b589	ffffff	Unknown
AAA	DMNPL1	000000000...	000000000...	Tue Dec 1...	34975770	ffffff	Unknown
AAA	DMNPL2	000000000...	A618B2F2...	Tue Dec 1...	34975743	ffffff	Unknown
ABC	DMNNT	078E9B46...	3739F5F75...	Mon Dec 2...	349e2c22	ffffff	Unknown
ABC	DMNPL1	D85774CF...	000000000...	Tue Dec 1...	34977974	ffffff	Unknown
ABC	DMNPL2	D85774CF...	1E35C64B...	Mon Dec 1...	34951282	ffffff	Unknown
ACURLY	DMNNT	078E9B46...	3739F5F75...	Mon Dec 2...	349e2c22	ffffff	Unknown
ACURLY	DMNPL1	078E9B46...	000000000...	Tue Dec 1...	3497794c	ffffff	Unknown
ACURLY	DMNPL2	078E9B46...	13B6928F9...	Fri Dec 12...	3490f36e	ffffff	Unknown
ADMIN	DMNNT	000000000...	000000000...	Sat Dec 13...	349247aa	ffffff	Unknown

User account flags to display

- Database changed
- Entry to be deleted
- Password missing
- New User to Sync
- DES Hash available
- MD4 Hash available
- Account Expired
- Account Locked Out
- Account Disabled
- Cannot Change Pwd

User account fields to display

- DES Hash
- MD4 Hash
- Timestamp 32-Bit (raw value)
- Timestamp 32-Bit (human form)
- Pwd Expiration Date (raw)
- Pwd Expiration Date (human)

Use this dialog to view the current state of the internal password synchronization database.

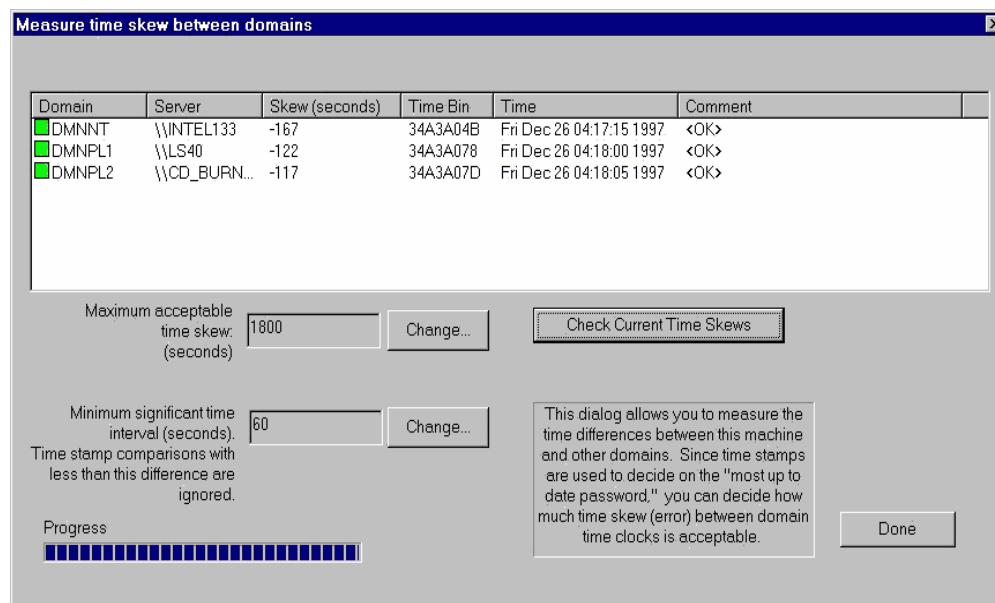
Sorting Order

- Sort by User
- Sort by Domain

Refresh Progress:

5. Time Skews

It would be very nice if all domain clocks were in perfect synchronization. Unfortunately, this is not the case. To deal with inaccuracies of time stamps, you can measure the time skew between domains and decide the minimum time difference to represent a new time stamp. You can specify the maximum error before time stamps will be ignored.



Our support staff is available to answer your technical questions whether you are a customer or not.

Voice: 800.829.6263 (USA/Canada) Voice: (01) 310.550.8575 (Worldwide) Fax: (01) 310.550.1152 (Worldwide)

Web: www.liebsoft.com Email: support@liebsoft.com

Microsoft
GOLD CERTIFIED
 Partner