

# Migration to Win 2K3

**Source:** <http://www.derkeiler.com/Newsgroups/microsoft.public.sqlserver.security/2005-10/0022.html>

---

**From:** mal hit (*malehit\_at\_yahoo.com*)

**Date:** 10/04/05

Date: Tue, 04 Oct 2005 08:30:54 -0700

Problem background:

We have a SQL Server 2000 database wherein we store encrypted data as well. Some of the data user enters via the web (password and security code) is encrypted using Windows 2000-based encryption. We decided to migrate from Windows 2000 to Windows 2003. However, we couldn't simply migrate the database because of the encrypted data. Win 2K uses DES-based encryption, while Win 2K3 uses AES. To resolve this problem we did the following:

1. Created a temporary table tblDataCopy:

```
Create table tblDataCopy
(
  Userid int,
  Win2KPwd varchar(6),
  Win2KPwdD varchar(6),
  Win2K3Pwd varchar(6),
  Win2K3PwdD varchar(6)
)
```

2. Copied Userid and Win2KPwd from the original table tblData. The web-based application stores Windows 2000-based encrypted data in column Win2KPwd.

3. Executed Windows 2000-based decryption logic on Win 2K and saved the decrypted data in column Win2KPwdD.

4. Moved the data over to a SQL Server 2000 database on Win 2K3.

5. Executed Windows 2003-based encryption logic on Win 2K3 to encrypt data in Win2KPwdD. This was saved in column Win2K3PwdD.

6. Executed Windows 2003-based decryption logic on Win 2K3 and saved the decrypted data in column Win2K3PwdD.

We expected that the data in columns Win2KPwdD and Win2K3PwdD would match. Much to our surprise, the encryption logic in Win 2K3 works in a

very 'inconsistent' manner. For instance, there are 250 rows with same data in Win2KPwdD. The data is '123456'. However, only 225 rows have the same decrypted data in Win2K3PwdD. The remaining 25 are either blank, NULL or 'incomplete' i.e. '123' or '12345' or '1234'.

No matter how many times we tried (from stored procs or VB code), the same records failed for the same reason on Win 2K3. We are following the same collation for both the databases.

Questions:

1. Is our approach to migrate the database from Win 2K to Win 2K3 correct?
2. Why doesn't Windows 2003-based encryption logic work consistently?
3. The encrypted data on Win 2K is stored in a varchar-based column. We never faced any problem encrypting/decrypting data on this OS. Is encryption on Win 2K3 Unicode-dependent? Even when we changed the column datatype to nvarchar, it didn't make any difference.
4. Is column length an issue on Win 2K3? Again, we didn't face any problems on Win 2K.
5. What other options are available to us?

Thanks a lot for your help.

\*\*\* Sent via Developersdex <http://www.developersdex.com> \*\*\*