

Requirements for running Dental 2000 on Windows 7

We recommend that the settings changes listed below be made by a PC technician or PC professional. Some of the changes involve using the Registry Editor, an area where serious damage can be done to your operating system if you do not know what you are doing.

1. Dental 2000 must be installed using the Dental 2000 install routine rather than copying the folders from an existing installation.
2. The shortcut for Dental 2000 must be set to run in XP SP3 compatibility mode.
3. All users running Dental 2000 must be "Administrator" type users
4. The CDSDATA folder where the data resides on the server must have full read/write permissions set.
5. The CDSW.ini file that resides in the Windows folder must have administrative rights.
6. Microsoft Security Essentials is incompatible with Dental 2000. It WILL cause the data to be corrupted! If Microsoft Security Essentials has been installed it must be uninstalled and replaced with some other virus protection such as Avast.
7. On all machines using Dental 2000, SMB2 must be turned off so that the system defaults to SMB (SMB1). This is relevant for Windows Vista and Windows Server 2008. At this time Windows 7 already uses SMB1 so this step is not necessary for Windows 7 users, although it may be in the future if Windows 7 is updated to use SMB2.

Disabling Oplocks on SMB2

Oplocks cannot be turned off for SMB2. You can apparently disable SMB2 itself, but how to do so is not documented by Microsoft and was only mentioned in a Microsoft support forum post as a workaround for a bug.

According to that post, SMB2 can be disabled on Windows operating systems that support it (Vista, Server 2008).

To disable SMB2 on a Windows Server 2008 or Windows Vista PC hosting embedded database tables, change or add the following Registry value:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters SMB2 = 0
```

Once SMB2 is disabled, SMB1 will be used again and the methods described below applied to disable oplocks for SMB1.

8. Oplocking must be disabled in the Registry

The Registry changes are listed in the format MainRegistryKey\SubKey\SubKey RegistryValue = RequiredValue where:

MainRegistryKey is one of the main Windows Registry keys (e.g. HKey_Local_Machine)

SubKey is any subkey of a main Registry key

RegistryValue is a Registry value to change or add in the specified Registry key

RequiredValue is the value RegistryValue must be set to cause the effect described

If any subkeys or values described do not exist in your Registry, you will have to add them. Please check carefully before doing so.

Disabling Oplocks on Windows Client PCs

To disable oplocks on a Windows client PC (a Windows PC that accesses an embedded database table hosted on another PC), change or add the following Registry values:

```
HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MRXSmb\Parameters OplocksDisabled = 1
```

Disabling Oplocks on Windows Servers

To disable oplocks on a Windows server (a Windows PC that hosts an embedded database table accessed from another PC), change or add the following Registry values:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters EnableOplocks = 0
```