

Windows Terminal Services and Citrix MetaFrame Support

Windows Terminal Services and Citrix MetaFrame support

Since the D2000 v7.00, release A040806039, D2000 system can operate in a terminal server environment - Windows Terminal Services. The processes with the graphic user interface ([D2000 CNF](#), [D2000 HI](#), [D2000 GrEditor](#)) have been modified. Processes can be started from a remote computer by means of Remote Desktop Connection (mstsc.exe application).

Since the D2000 v7.0, release A050415070, D2000 system is able to work in the environment of Citrix MetaFrame Presentation Server. The processes with the graphic user interface ([D2000 CNF](#), [D2000 HI](#), [D2000 GrEditor](#)) have been modified. Processes can be started from a remote computer by means of ICA Client (tested on *Citrix MetaFrame Presentation Server* (server) v 3.0 and *ICA Client* (client) v 8.00.24737 and v 9.150.39151).

In the Windows Terminal Services or Citrix MetaFrame environments, the above-mentioned user processes change their behaviour according to following specifications:

- They change their names (analogous to starting them using the parameter [/W](#)) to the name of the computer, from which the client is connected (e.g. Workstation1.CNF)
- If not explicitly specified otherwise, they connect to the process [D2000 Server](#) via TCP protocol instead of the shared memory (shared memory is not global and therefore it does not work in the Windows Terminal Services and Citrix MetaFrame environment)
- They read a [hardware key](#) from the client computer. If several hardware keys are plugged into the client computer, only the key with the highest privileges is read. If a user process was started in the Windows Terminal Services or Citrix MetaFrame environments and it read the hardware key, the process will regularly detect whether the connection to the client computer is active. If the connection fails and it is not recovered within 1 minute, the user process displays an error message and will be terminated.
- If [Enhanced security](#) is part of your D2000 system licence, the process [D2000 HI](#) reads a **logon key** (security token) from client computer. Logon key is necessary for user to log on to a D2000 system with *Enhanced security* enabled.

The above-mentioned enhancements facilitate the following operations:

- A large number of clients (operators - HI, application engineers - CNF, etc.) can work on one Windows server, that may but does not have to be a server where [D2000 Server](#) is running. To increase the security (to prevent the intentional attack of the computer where [D2000 Server](#) is running by its clients, damage by viruses, ...) you can e.g. separate this terminal server from the [D2000 Server](#) by means of a firewall, keep only the ports required for communication accessible and block the other services.
- Remote configuration of the D2000 system (via Internet or modem) - CNF [Hardware key](#) does not have to be plugged into the server.
- Remote management of the D2000 system (Remote Desktop Connection allows you not only to create a new session, but also connect to the server console and subsequent interaction with running applications)

A *wtstd21.dll* library, distributed with D2000 version 7.02.006 and higher (with newer date than 24.09.2008), enables the transfer of client computer name, hardware key and logon key via several Windows Terminal Services / Citrix MetaFrame connections.

E.g. a *Remote Desktop* connection from the client computer *Workstation1* can be open to computer *Server1*. From there another *Remote Desktop* connection can be open to computer *Server2*, where HI process has been started. This HI process will change its name to *Workstation1.HIP*.

The new *wtstd21.dll* library is compatible with old library, i.e. it is not necessary to upgrade D2000 but the replacement of old library with a new one is sufficient. The replacement must be performed on all computers "on the way" with the exception of the first one and the last one (there the replacement is optional). In the mentioned example it would be necessary to replace only *wtstd21.dll* library on computer *Server1*.

Note: All above mentioned functionality is facilitated by *wtstd21.dll* library integrated on client's side. If the library is not present on client's side or the connection to Windows Terminal Server is established from Windows CE client or the connection to Citrix MetaFrame Server from Unix client (in both cases the library *wtstd21.dll* is unusable), this minimal functionality is still available:

- the processes change their names (analogous to starting them using the parameter [/W](#)) to the name of the computer, from which the client is connected (e.g. Workstation1.CNF),
- if not explicitly specified otherwise, the processes connect to the process [D2000 Server](#) via TCP protocol instead of the shared memory (shared memory is not global and therefore it does not work in the Windows Terminal Services and Citrix MetaFrame environment).

Configuration of Windows Terminal Services client

To work in the Windows Terminal Services environment, the *wtstd21.dll* library must be installed on the client computer (i.e. the computer, from which the user is connected to the target Windows Server by means of a modem, local network or Internet). The library is installed automatically when installing the D2000 system, but it also can be installed manually (i.e. no need to install D2000 system on the client computer) as follows:

- Copy the files *wtstd21.dll* and *sx32w.dll* to the system directory (by default **C:\windows\system32**). The file *wtstd21.dll* is located in the system directory of a computer with a D2000 system installation; the file *sx32w.dll* is located in the [installation directory](#) of the D2000 system.
- Using the program **regedit**, create the following key in the registry:
HKEY_CURRENT_USER\Software\Microsoft\Terminal Server Client\Default\AddIns\WTSD21
and then the value of String type named **Name** and the value of *wtstd21.dll* in the key
- If this procedure has been performed correctly, the file *wtstd21.log* will be created in the directory **%TEMP%** after starting the Remote Desktop Connection and connecting a Windows Server.
Note: Prior to version D2000 7.1.21 the log was created in the current directory of the running program. In previous example it would be C:\windows.

Besides the *wtstd21.dll* library, you must install a Sentinel driver for [hardware keys](#) on the client computer (i.e. the computer with the hardware keys), otherwise the hardware and logon key reading will not work.

If the information about the hardware key are transmitted via more servers (e.g. the situation in which the user starts Remote Desktop Connection within the other Remote Desktop Connection session), the *wtstd21.dll* library must be installed on the each server through which the connection is done.

Note 1: Starting with D2000 Version 8, a 64-bit Version of *wtstd21_64.dll* is available. It can be integrated to 64-bit Remote Desktop client in 64-bit Windows environment. Integration can be performed manually using the procedure described above (only the value of String type named **Name** will be **wtstd21_64.dll**).

The 64-bit version of library *sx32w.dll* must be copied too. Please remember that copying must be performed in 64-bit application (e.g. Windows Explorer and not 32-bit Total Commander), as the directory displayed in 64-bit Windows by a 32-bit application as *C:\WINDOWS\system32* is in fact *C:\WINDOWS\SysWOW64* (Windows on 64-bit Windows) - feature called *File system redirection*. So even after the libraries are copied they won't be visible in *C:\WINDOWS\system32* in 32-bit applications.

Note 2: Starting with D2000 Version 8.00.008, an installation cabinet installs these *dll* files. It inserts the 64-bit Version of *wtstd21.dll* and *sx32w.dll* files into the directory **Bin64**. This directory also contains the file *xcopy64.exe* to copy both files into own directory. For example: *xcopy64 wtstd21.dll c:\windows\system32*

Configuration of Citrix MetaFrame Presentation Server client

To work in the Citrix MetaFrame environment, Citrix ICA Client software must be installed on client computer (i.e. computer, from which the user is connected to the Citrix MetaFrame Presentation Server by means of a modem, local network or Internet). The *wtstd21.dll* library must be automatically or manually (using Citrix administrative tools) registered to the client. Manual registration of the library is, as follows:

- Copy the *wtstd21.dll* file to the directory where the Citrix ICA Client software was installed in (by default *C:\Program Files\Citrix\ICA Client*). The *wtstd21.dll* file is located in the system directory of the computer where D2000 system was installed in.
- Modify the *module.ini* configuration file located in the directory where Citrix ICA Client was installed in (by default *C:\Program Files\Citrix\ICA Client*):
 - in the *[ICA 3.0]* section, the row *VirtualDriver =* add *D2Drv* to the end of the following row:

```
VirtualDriver = Thinwire3.0,ClientDrive,ClientPrinterQueue,ClientPrinterPort,Clipboard,
ClientComm,ClientAudio,ClientManagement,LicenseHandler,ProgramNeighborhood,TWI,ZL_FONT,ZLC,SmartCard,
Multimedia,ICACTL,SpeechMike,SSPI,D2Drv
```

- in the *[VirtualDriver]* section, add the following row:

```
D2Drv =
```

- add the following section to the end of *module.ini* file:

```
[D2Drv]
DriverName      = WTSD21.DLL
DriverNameWin16 = WTSD21.DLL
DriverNameWin32 = WTSD21.DLL
```

- If the above instructions are performed correctly, the *wtstd21.log* file will be generated in the directory **%TEMP%** after starting Citrix ICA Client.
Note: Prior to version D2000 7.1.21 the log was created in the current directory of running program. In previous example it would be *C:\Program Files\Citrix\ICA Client*.

Besides the *wtstd21.dll* library, you must install a Sentinel driver for hardware keys on the client computer (otherwise hardware and logon key reading will not work).

Note: Starting with D2000 version 7.02.005, the following feature is supported: if the *wtstd21.dll* library is not registered in Citrix ICA Client environment, the processes with the graphic user interface will query the name of the client computer by using Citrix API and they'll change their names to the name of the computer, from which the client is connected (e.g. MYCOMP.HIP). This enables to run D2000 processes from client computers for which the library *wtstd21.dll* is not available (Windows CE, various Unix clones etc).

Change of the logon key search interval

If **Enhanced security** is part of D2000 system licence and the process **D2000 HI** has read a **logon key** (security token), the process checks the presence of the key each 60 seconds. The interval may be changed using the program *regedit* - create the new value **RemoteHwKeyWD** of *DWORD* type in the key **HKEY_LOCAL_MACHINE\SOFTWARE\Ipssoft\D2000V70** and set it to required time interval (seconds).