Administrating DriveWindow 2

Table of Contents

1. PREFACE 3
1.1. PURPOSE 3
1.2. PRODUCT 3
1.3. DEFINITIONS, TERMINOLOGY AND ABBREVIATIONS 3
1.4. REFERENCES AND RELATED DOCUMENTS 11

2. GENERAL DESCRIPTION 12
2.1. ENVIRONMENT 12
2.1.1. Users 12
2.1.2. Local and Remote Use 12
2.1.3. Drive Communication 12
2.1.4. Drive 12
2.1.5. Other Software 12
2.2. GENERAL RESTRICTIONS 13
2.3. ASSUMPTIONS AND DEPENDENCIES 13

3. NETWORKS 13
3.1. INTRANET 13
3.2. VIRTUAL PRIVATE NETWORK 14
3.3. INTERNET 14
3.4. CONNECTIONS 15

4. SYNCHRONIZATION OF MULTIPLE ACCESS 15
4.1. SYSTEM SOFTWARE 16
4.2. DRIVE RESOURCES 16

5. DRIVEWINDOW ARCHITECTURE 17
5.1. LOCAL 17
5.2. REMOTE 17
5.3. OFF-LINE 18

6. INSTALLATION 18
6.1. INSTALLATION FOLDER 18
6.2. FILE AND FOLDER ACCESS RIGHTS 18
6.3. REGISTRY CHANGES 20

7. LOCAL USE 21

8. REMOTE USE 23

8.1. INSTALLING FOR REMOTE USE 24

8.2. CONFIGURING THE REMOTE END 24

8.2.1. Some Assumptions 25

8.2.2. Users 28

8.2.3. Right to Access the Remote Computer from Network 29

8.2.4. Adding a Special Account for the Remote OPC Server 30

8.2.5. Configuring the Remote End OPC Server 32

8.3. CONFIGURING THE CLIENT END 40

8.4. AUDITING THE REMOTE END 41

8.4.1. Configuring for Audit 41

8.5. SIMULTANEOUS LOCAL AND REMOTE USE 45

8.5.1. Denying Local Use at Remote End 46

8.5.2. Forcing Remote Use instead of Local Use at the Remote End 46

8.6. PRE-DEFINED REMOTE USE INSTEAD OF LOCAL USE 46

8.7. USING IN-PROCESS SERVER AT THE REMOTE END 46

9. EXTERNAL REFERENCES 46

10. OTHER FEATURES 46

10.1. PERFORMANCE 46

10.2. USABILITY, RECOVERY, SAFETY AND PROTECTION 47

10.3. MAINTENANCE 47

10.4. PORTABILITY AND COMPATIBILITY 47

1. Preface

This document contains administration instructions of the 32-bit **DriveWindow** (version 2.10 or newer) for Windows NT.

1.1. Purpose

DriveWindow is needed to make commissioning, maintenance, and debugging of drives and drive systems fast and easy.

1.2. Product

DriveWindow for NT is a 32-bit Windows program running under Windows NT 4.0 SP3 (or newer), Windows 2000, or Windows XP operating system in a x86 PC.

1.3. Definitions, Terminology and Abbreviations

Access	Access is simply being able to get to what you need.
Account	See User Account; Group Account.
ActiveX	A set of technologies that enables software components to interact with one another in a networked environment, regardless of the language in which they were created. ActiveX™ is built on the Component Object Model (COM).
Administrative Account	An account that is a member of the Administrators local group of a computer or domain.
Administrator	A person responsible for setting up and managing domain controllers or local computers and their user and group accounts, assigning passwords and permissions, and helping users with networking issues. To use administrative tools such as User Manager or User Manager for Domains, an administrator must be logged on as a member of the Administrators local group of the computer or domain, respectively.
Administrator Privilege	One of three privilege levels you can assign to a Windows NT user account. Every user account has one of the three privilege levels (Administrator, Guest, and User).
AMC	Application and Motor Controller.
Architecture	In information technology, especially computers and more recently networks, architecture is a term applied to both the process and the outcome of thinking out and specifying the overall structure, logical components, and the logical interrelationships of a computer, its operating system, a network, or other conception.
Authentication	Authentication is the process of determining whether someone or something is, in fact, who or what it is declared to be.

Backup	The activity of copying files or databases so that they will be preserved in case of equipment failure or other catastrophe.
Browse	To view available items by looking through lists of folders, files, user accounts, groups, domains, computers, etc.
Click	To press and release a mouse button quickly.
Client	An object that requests services from another object.
COM	An open architecture for cross-platform development of client/server applications based on object-oriented technology as agreed upon by Digital Equipment Corporation and Microsoft Corporation. The Component Object Model defines an interface (similar to an abstract base class), IUnknown, from which all COM-compatible classes are derived.
Component	In object-oriented programming and distributed object technology, a component is a reusable program building block that can be combined with other components in the same or other computers in a distributed network to form an application.
Computer	A device that accepts information (in the form of digital data) and manipulates it for some result based on a program or sequence of instructions on how data is to be processed.
Computer Name	A unique name of up to 15 uppercase characters that identifies a computer to the network. The name cannot be the same as any other computer or domain name in the network
Datagram	A self-contained, independent entity of data carrying sufficient information to be routed from the source to the destination computer without reliance on earlier exchanges between this source and destination computer and the transporting network.
DCOM	Distributed Component Object Model. An object protocol that enables ActiveX™ components to communicate directly with each other across a network. DCOM is language neutral, so any language that produces ActiveX components can also produce DCOM applications.
DDCS	Distributed Drives Communication Circuit.
DDCS protocol	Communication protocol used in ACS600 products.
Device	In the context of computer technology, a device is a unit of hardware, outside or inside the case or housing for the essential computer (processor, memory, and data paths) that is capable of providing input to the essential computer or of receiving output or of both.
Dialog Box	A window that is displayed to request or supply information.
Disabled User Account	A user account that does not permit logons. The account appears in the user account list of the User Manager or User Manager for Domains window and can be re-enabled at any time

Domain	A sphere of knowledge identified by a name. Typically, the knowledge is a collection of facts about some program entities or a number of network points or addresses. In Windows NT, a collection of computers defined by the administrator of a Windows NT Server network that share a common directory database. A domain provides access to the centralized user accounts and group accounts maintained by the domain administrator. Each domain has a unique name.
Downloading	The transmission of a file from one computer system to another, usually smaller computer system
Drive	Equipment that converts electric to mechanical power.
Drive Controller	A board or a device that is used to control a drive.
Dynamic-Link Library (DLL)	An operating system feature which allows executable routines (generally serving a specific function or set of functions) to be stored separately as files with DLL extensions and to be loaded only when needed by the program that calls them.
Firewall	Or proxy server. A system or combination of systems that enforces a one-way barrier between two or more networks, usually used for security purposes. Firewalls accomplish all communication between the network and outside.
Folder	A grouping of files or other folders, graphically represented by a folder icon,
Group	In User Manager or User Manager for Domains, an account containing other accounts that are called members. The permissions and rights granted to a group are also provided to its members, making groups a convenient way to grant common capabilities to collections of user accounts. For Windows NT Workstation, groups are managed with User Manager. For Windows NT Server, groups are managed with User Manager for Domains.
Group Account	A collection of user accounts. Giving a user account membership in a group gives that user all the rights and permissions granted to the group
Group Memberships	The groups to which a user account belongs. Permissions and rights granted to a group are also provided to its members. In most cases, the actions a user can perform in Windows NT are determined by the group memberships of the user account the user is logged on to
Group Name	A unique name identifying a local group or a global group to Windows NT. A group's name cannot be identical to any other group name or user name of its own domain or computer.
Guest Account	On computers running Windows NT Workstation or Windows NT Server, a built-in account used for logons by people who do not have a user account on the computer or domain or in any of the domains trusted by the computer's domain.

Guest Privilege	One of three privilege levels that you can assign to a Windows NT user account.
Impersonation	Impersonation occurs when Windows NT Server allows one process to take on the security attributes of another
In-process server	An object server implemented as a DLL that runs in the process space of the object's client.
Instance	An object for which memory is allocated or which is persistent.
Interactive Logon	A network logon from a computer keyboard, when the user types information in the Logon Information dialog box displayed by the computer's operating system
Internet	A collection of computer networks that connects millions of computers around the world.
Intranet	A network within an organization, usually connected to the Internet via a firewall.
IP	Internet Protocol. The messenger protocol of TCP/IP, responsible for addressing and sending TCP packets over the network. IP provides a best-effort, connectionless delivery system that does not guarantee that packets arrive at their destination or that they are received in the sequence in which they were sent.
ISA	Industry Standard Architecture. A standard bus (computer interconnection) architecture that is associated with the IBM AT motherboard.
ISP	A company that provides access to end users of the Internet.
LAN	Local Area Network. A group of computers and other devices dispersed over a relatively limited area and connected by a communications link that enables any device to interact with any other on the network.
Link	1) Using hypertext, a link is a selectable connection from one word, picture, or information object to another. 2) In telecommunications, a link is a physical (and, in some usages, a logical) connection between two points.
Local Group	For Windows NT Workstation, a group that can be granted permissions and rights only for its own workstation. However, it can contain user accounts from its own computer and (if the workstation participates in a domain) user accounts and global groups both from its own domain and from trusted domains.
Log on	To provide a user name and password that identifies you to the network.
Menu	A list of available commands in an application window. Menu names appear in the menu bar near the top of the window.

Modbus protocol	A local area network system for industrial control applications. The Modbus protocol was developed by Modicon (part of Schneider Automation).
Module	In computers, in general, a separate unit of software or hardware.
Monitoring	The act of detecting the presence of signals and the measurement thereof with appropriate measuring instruments.
Network	A series of points or nodes interconnected by communication paths. Networks can interconnect with other networks and contain subnetworks.
Object	A programming structure encapsulating both data and functionality that are defined and allocated as a single unit and for which the only public access is through the programming structure's interfaces.
OLE	Pronounced o-LAY. A way to transfer and share information between applications.
OPC	OLE for Process Control. An emerging software technology standard (http://www.opcfoundation.org/) that connects Windows-based process control systems to hardware devices on the plant floor. This technology provides a common interface to different hardware devices, allowing process control applications to communicate with broad set of devices.
Pass-through Authentication	When the user account must be authenticated, but the computer being used for the logon is not a domain controller in the domain where the user account is defined, nor is it the computer where the user account is defined, the computer passes the logon information through to a domain controller (directly or indirectly) where the user account is defined.
Password	A password is an unspaced sequence of characters used to determine that a computer user requesting access to a computer system is really that particular user.
PC	Personal Computer.
PCMCIA	Personal Computer Memory Card International Association. An industry group organized in 1989 to promote standards for a credit card-size memory or I/O device that would fit into a personal computer, usually a notebook or laptop computer.
PDF	Portable Document Format. A file format that has captured all the elements of a printed document as an electronic image that you can view, navigate, print, or forward to someone else. PDF files are created using Adobe Acrobat, Acrobat Capture, or similar products.
Permissions	Windows NT Server settings you set on a shared resource that determine which users can use the resource and how they can use it.
Persistent	Lasting between program sessions, or renewed when a new program session is begun.

Plug and Play (PnP)	Gives computer users the ability to plug a device into a computer and have the computer recognize that the device is there. The user does not have to tell the computer.
PPTP	Point-to-Point Tunneling Protocol. A newer networking protocol that enables remote users to access corporate networks securely across the Internet by dialing into an Internet service provider (ISP) or by connecting directly to the Internet. PPTP supports multiprotocol virtual internal networks (VPNs). Because PPTP allows multiprotocol encapsulation, users can send any packet type over an IP network.
Privilege Level	One of three settings (User, Administrator, or Guest) assigned to each user account. The privilege level a user account has determines the actions that the user can perform on the network.
Process	When a program runs, a Windows NT process is created. A process is an object type which consists of an executable program, a set of virtual memory addresses, and one or more threads
Property	The data associated with an object (same as Attribute).
Protocol	In networking, a formal set of rules governing the format, timing, sequencing, and error control of exchanged messages on a data network; may also include facilities for managing a communications link and/or contention resolution; a protocol may be oriented toward data transfer over an interface, between two logical units directly connected, or on an end-to-end basis between two end users over a large and complex network.
Proxy	An interface-specific object that provides the parameter marshaling and communication required for a client to call an application object that is running in a different execution environment, such as on a different thread or in another process. The proxy is located with the client and communicates with a corresponding stub that is located with the application object that is being called.
Registry	In the Microsoft Windows operating systems, the Registry is a single place for keeping such information as what hardware is attached, what system options have been selected, how computer memory is set up, and what application programs are to be present when the operating system is started.
Remote Logon	Occurs when a user is already logged on to a user account and makes a network connection to another computer.
Remote Procedure Call (RPC)	A message-passing facility that allows a distributed application to call services available on various machines in a network. Used during remote administration of computers.
Security	A means of ensuring that shared resources can be accessed only by authorized users
Security Log	Records security events. This helps track changes to the security system and identify any possible breaches of security.

Security Policies	For Windows NT Workstation, the security policies consist of the Account, User Rights, and Audit policies, and are managed using User Manager.
Select	To mark an item so that a subsequent action can be carried out on that item. You usually select an item by clicking it with a mouse or pressing a key. After selecting an item, you choose the action that you want to affect the item.
Semaphore	In programming, especially in UNIX systems, a semaphore is a technique for coordinating or synchronizing activities in which multiple processes compete for the same operating system resource.
Server	An object that responds to a client request or, in a network, any device that can be shared by all users.
Service	A process that performs a specific system function and often provides an application programming interface (API) for other processes to call. Windows NT services are RPC-enabled, meaning that their API routines can be called from remote computers.
Service Pack	An update to the operating system or application software.
SP	Service Pack.
Stub	An interface-specific object that provides the parameter marshaling and communication required for an application object to receive calls from a client that is running in a different execution environment, such as on a different thread or in another process. The stub is located with the application object and communicates with a corresponding proxy that is located with the client that calls it.
Task Manager	Task Manager enables you to start, end, or run applications, end processes (either an application, application component, or system process), and view CPU and memory use data. Task Manager gives you a simple, quick view of how each process (application or service) is using CPU and memory resources
TCP	Transmission Control Protocol. A connection-based Internet protocol responsible for breaking data into packets, which the IP protocol sends over the network. This protocol provides a reliable, sequenced communication stream for network communication.
TCP/IP	Transmission Control Protocol/Internet Protocol. A set of networking protocols that provide communications across interconnected networks made up of computers with diverse hardware architectures and various operating systems. TCP/IP includes standards for how computers communicate and conventions for connecting networks and routing traffic.
Thread	Threads are objects within processes that run program instructions. They allow concurrent operations within a process and enable one process to run different parts of its program on different processors simultaneously.

Trend	To show a tendency.
Trust Relationship	A link between domains that enables pass-through authentication, in which a trusting domain honors the logon authentications of a trusted domain. With trust relationships, a user who has only one user account in one domain can potentially access the entire network. User accounts and global groups defined in a trusted domain can be given rights and resource permissions in a trusting domain, even though those accounts don't exist in the trusting domain's directory database.
Trust Relationships Policy	A security policy that determines which domains are trusted and which domains are trusting domains. See also Trust Relationship.
Trusted Domains	See Trust Relationship.
UDP	User Datagram Protocol. A communications method (protocol) that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP).
Uploading	The transmission of a file from one computer system to another, usually larger computer system.
User Account	Consists of all the information that defines a user to Windows NT. This includes such things as the user name and password required for the user to log on, the groups in which the user account has membership, and the rights and permissions the user has for using the system and accessing its resources. For Windows NT Workstation, user accounts are managed with User Manager. For Windows NT Server, user accounts are managed with User Manager for Domains.
User Manager	A Windows NT Workstation tool used to manage the security for a workstation. User Manager administers user accounts, groups, and security policies.
User Name	A unique name identifying a user account to Windows NT. An account's user name cannot be identical to any other group name or user name of its own domain or workgroup.
User Password	The password stored in each user's account. Each user generally has a unique user password and must type that password when logging on or accessing a server.
User Privilege	One of three privilege levels you can assign to a Windows NT user account. Every user account has one of the three privilege levels (Administrator, Guest, and User). Accounts with User privilege are regular users of the network; most accounts on your network will probably have User privilege.
User Rights	Define a user's access to a computer or domain and the actions that a user can perform on the computer or domain. User rights permit actions such as logging onto a computer or network, adding or deleting users in a workstation or domain, and so forth.
User Rights Policy	Manages the assignment of rights to groups and user accounts.

VPN	Acronym for virtual private network, a remote LAN that can be accessed through the Internet using the new PPTP.
Web	Or the World Wide Web. The portion of the global Internet that uses hypertext links to connect pages and resources in a way that lets you reach any page from any other page.
Window	A rectangular area on your screen in which you view an application or document.
Window Station	In Windows NT, a secure object that contains a clipboard, a set of global atoms and a group of desktop objects. The interactive window station assigned to the logon session of the interactive user also contains the keyboard, mouse, and display device. The interactive window station is visible to the user and can receive input from the user. All other window stations are noninteractive, which means that they cannot be made visible to the user, and cannot receive user input.
Windows NT	An operating system made by Microsoft. Rumors has it that NT stands for "New Technology". The fact is that NT was born from a project led by David Cutler, formelly DEC's researcher, hired by Microsoft in 1988 specially to devellop a new outstanding operating system. At DEC, Cutler had created several operating systems, including the very famous VMS (now called OpenVMS) from which NT has inherited some features such as process' priority levels and dynamic working set trimming. Some people say that the name Windows NT (WNT) was derived by taking the next letters of V, M and S, respectivelly. You can reach Cutler's unnoficial fan club at http://web.wt.net/~shannonh. The OpenVMS home page can be found at http://www.digital.com/openvms. I have used VMS and NT for several years, so I can tell you: they both are really fantastic! The very first commercial version of NT appeared in 1993, and was called Microsoft Windows NT 3.1. Following that we had the versions 3.5 (1994), 3.51 (1995) and 4.0 (1996). The next version of NT (5.0) will probably come in the first half of 1999, and you can expect a great deal of changes in this really new version. Check this information at http://www.microsoft.com/ntserver. (Source: http://www.netcettera.com.br/history.htm)
Workstation	Any networked computer using server resources
x86	A generic name for the series of Intel microprocessor families that began with the 80286 microprocessor.

1.4. References and Related Documents

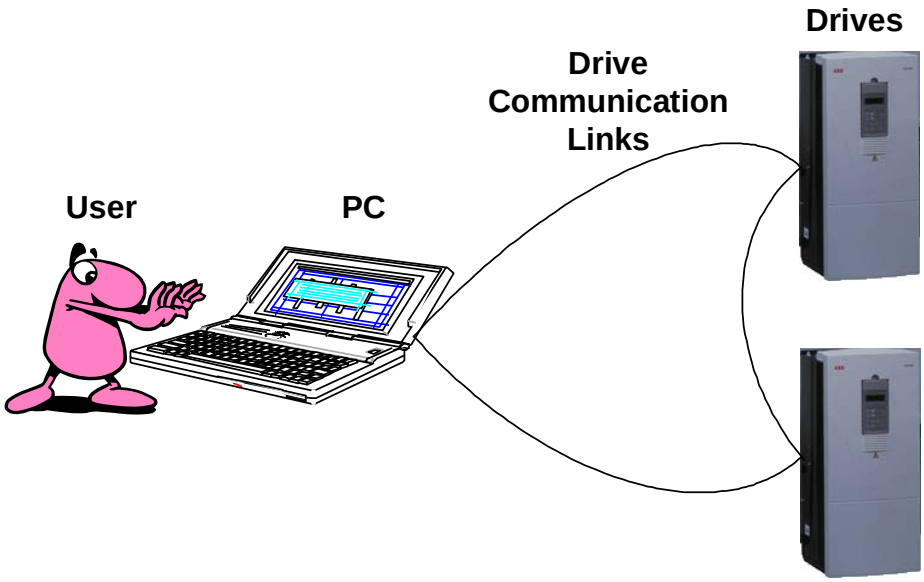
DRIVEWINDOW 2.0 USER MANUAL (PDM VaultID=00026315.DOC)/99-04-22 by Aki Kolehmainen)

DRIVEWINDOW 2.X FUNCTIONAL SPECIFICATION (PDM VaultID=00027533.DOC)/99-07-06 by Jyrki Erjanti)

2. General Description

2.1. Environment

DriveWindow environment consists of User, PC or two PCs connected through a network, Drive Communication Links, and Drive Controllers (Drives).



Local Use

2.1.1. Users

Users of DriveWindow are ABB personnel and ABB customers commisioning and maintaining ABB made drives.

2.1.2. Local and Remote Use

Because Microsoft COM (DCOM) technology is used in implementing DriveWindow, it is possible to use DriveWindow locally as well as remotely through all kind of networks that Microsoft DCOM technology can handle.

2.1.3. Drive Communication

DriveWindow supports optical links through ISA or PCMCIA cards using DDCS protocol.

2.1.4. Drive

Drive or Drive Controller is a device that is the target for commissioning or maintenance.

2.1.5. Other Software

DriveWindow provides COM and OPC based Application Interfaces for use by other programs.

2.2. General Restrictions

Only English version of the program is available and there is no provision for translations into other languages.

2.3. Assumptions and Dependencies

DriveWindow implementation is modular. Implementation and interfaces are based on existing standards (ActiveX, OPC, COM, DCOM).

3. Networks

Because Microsoft COM (DCOM) technology has been used in implementing DriveWindow, it is possible to use DriveWindow remotely through all kind of networks that Microsoft DCOM technology can handle.

Using DriveWindow over a network requires that system administrators do proper settings (user accounts, security settings, firewalls) possibly at both ends, but specially at the remote end.

Firewall settings are out of the scope of this paper and are not explained here, but it is not a trivial matter.

More information about DCOM is in DCOM Technical Overview, for example. It can be found at:

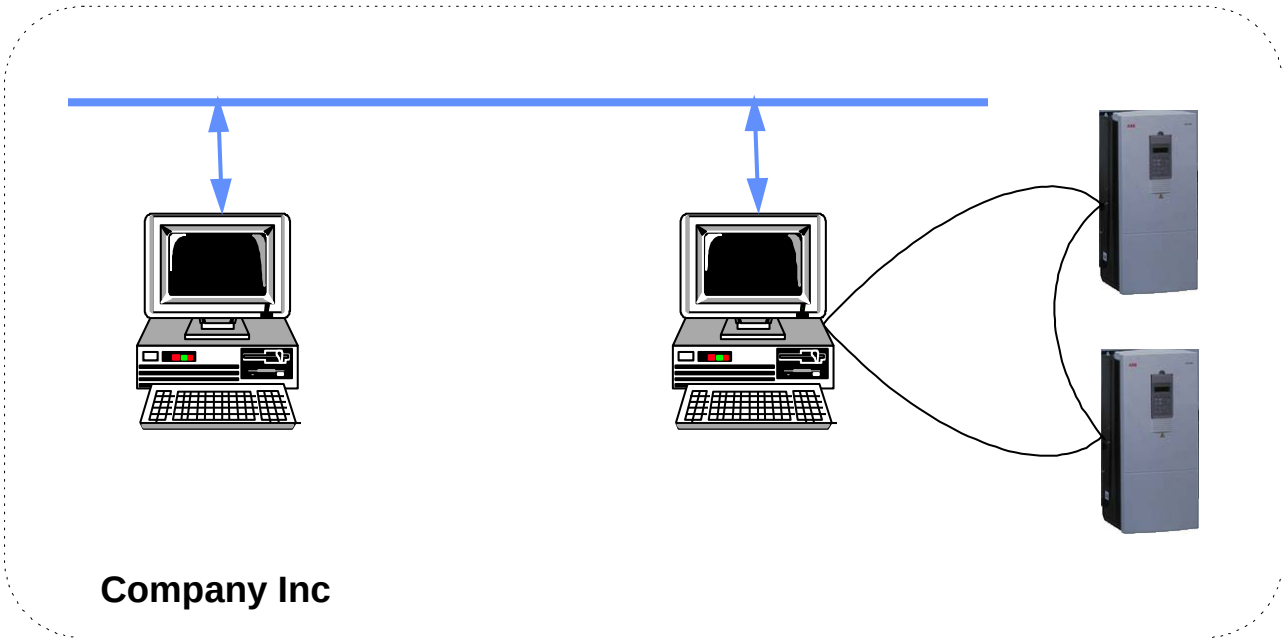
http://msdn.microsoft.com/library/en-us/dndcom/html/msdn_dcomtec.asp

Information about configuring firewalls for DCOM is in Using Distributed COM with Firewalls, for example. It can be found at:

http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomfirewall.asp

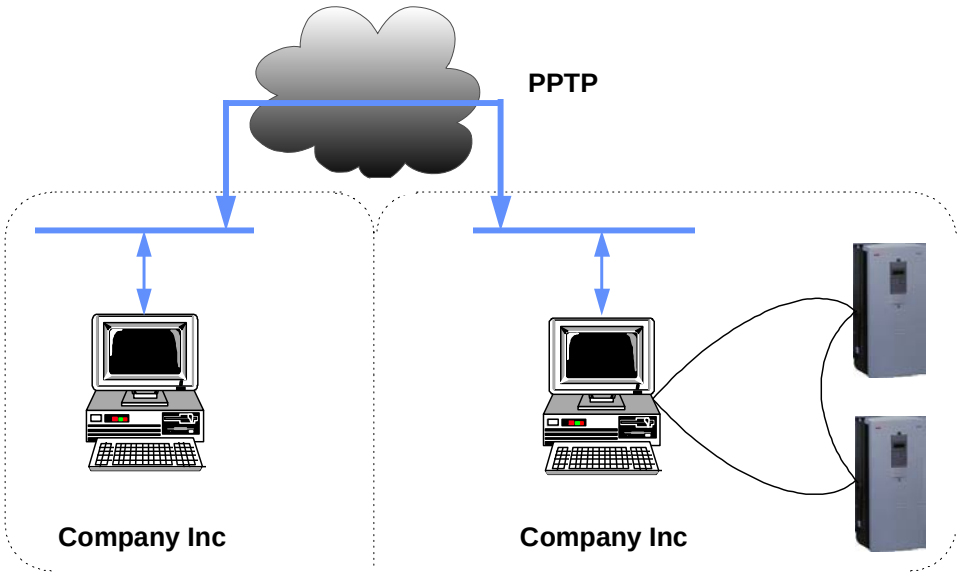
3.1. Intranet

Setting up DCOM over intranet is perhaps the easiest way to use DriveWindow remotely.



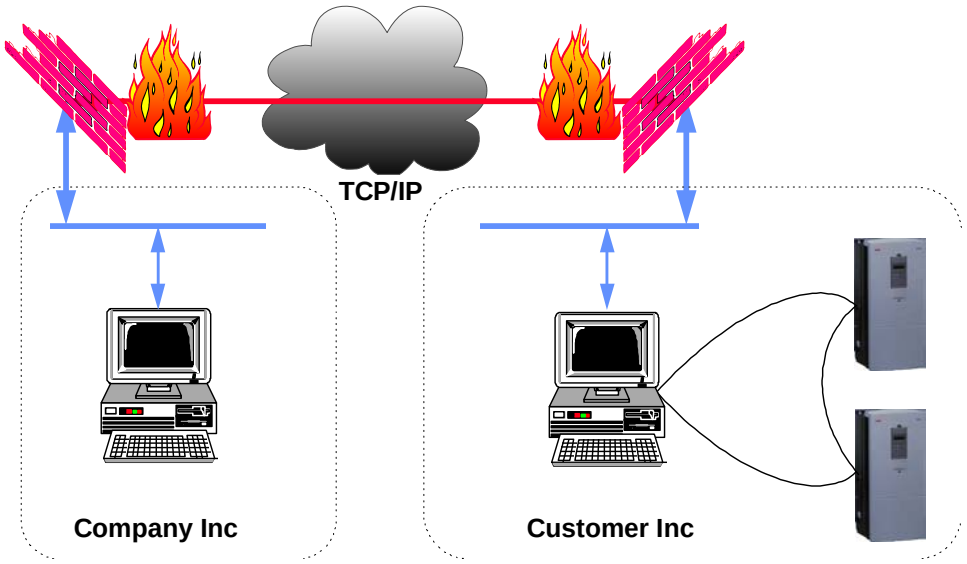
3.2. Virtual Private Network

Virtual private networks such as the Windows NT 4.0 Point-to-Point Tunnelling Protocol (PPTP) are one way of using the network to securely tunnel private information over the Internet. DCOM-based applications such as DriveWindow can transparently leverage such a virtual private network.



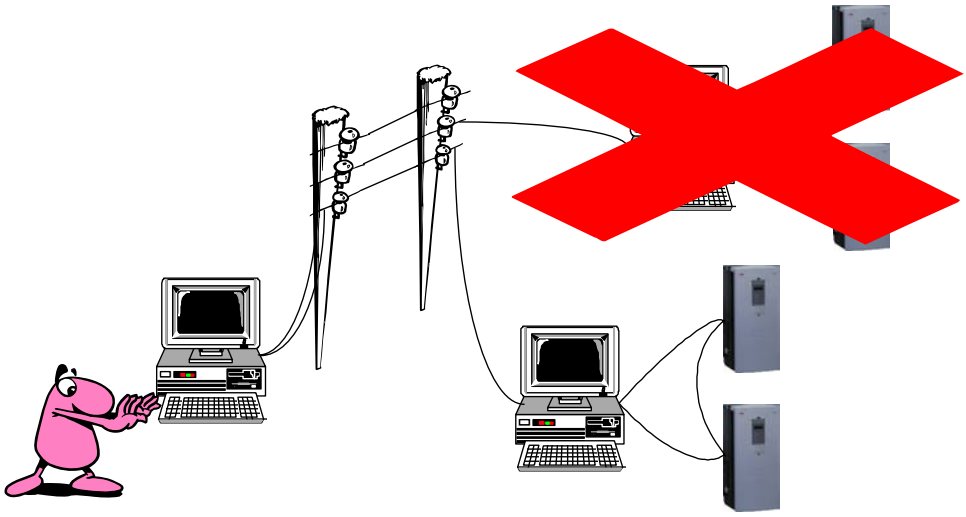
3.3. Internet

Using DCOM over internet usually involves firewalls at both ends. It means that firewalls have to be configured for DCOM as well (see http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dndcom/html/msdn_dcomfirewall.asp). Security may also be degraded.



3.4. Connections

DriveWindow supports only one connection at a time, whether local or remote. It means that it is not possible to collect data simultaneously through two different remotely connected PCs, for example.



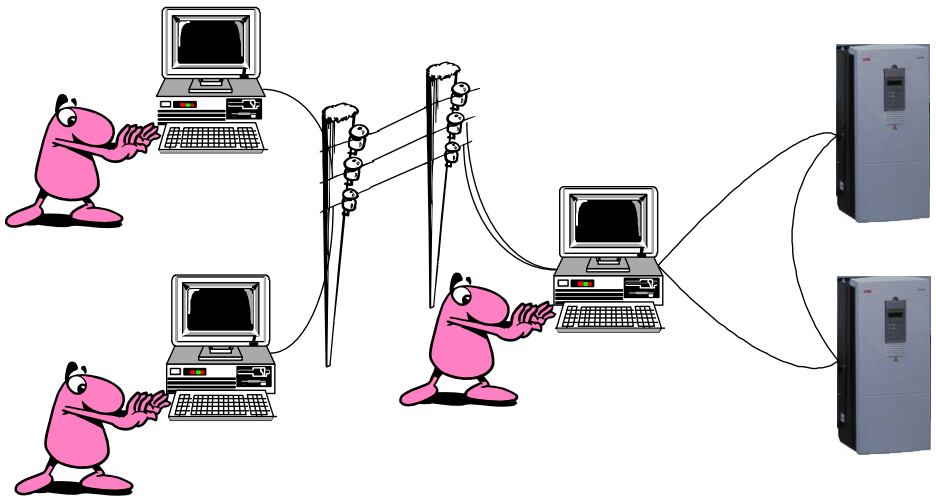
The connection to be done is asked when DriveWindow starts. There is also a menu command to do the connection. The user has the choice to select the local computer or enter the name or address of a remote computer.

A connected DriveWindow can be disconnected by a menu command. Disconnection must be made before a new connection can be made. Disconnection is automatically done when DriveWindow exits.

Disconnection closes or clears all windows that contain drive data.

4. Synchronization of Multiple Access

There may be several different applications, or more than one DriveWindow (perhaps running remotely) that try to use the communication links simultaneously. Access to the drives is internally synchronized so that the applications do not crash when accessing a drive.



In the Communication Library there is a global semaphore, which is used to deny access to the drive communication links from all but one application running simultaneously. DriveWindow 2 does not show any error messages to the user if there is a denial, but it shows no drives in this case. Since version 2.01, a message box is shown, which tells that another process is using the hardware. However, because the communication library displays it, it is not shown in case of remote access.

If the remote end computer is configured properly, all users share the same DriveOPC, which allows simultaneous access to the drives. If all users use DriveWindow 2 as the client, only one user can use the server. All other user get an error message when trying to connect. If other programs than DriveWindow 2 are used as the client, users must be aware that at the same time she is working, some other user may compete in changing parameter values.

4.1. System Software

System Software can be backed up, restored, and downloaded locally as well as remotely.

When done remotely, or even locally on a computer being used as remote end as well, extra care has to be taken, if simultaneous access by several users is possible.

While system software is uploading or downloading, no other user should access that drive. Other drives on the drive communication links can be accessed, although the limited bandwidth of the communication links severely degrades the performance.

There is no internal synchronization of accessing a drive while system software is uploading or downloading. It means that if the configuration allows simultaneous access, the users must agree upon some synchronization policy by themselves.

4.2. Drive Resources

Use of drive resources, such as data loggers, control point, and parameter values, remotely, or even locally on a computer being used as remote end as well, extra care has to be taken, if simultaneous access by several users is possible.

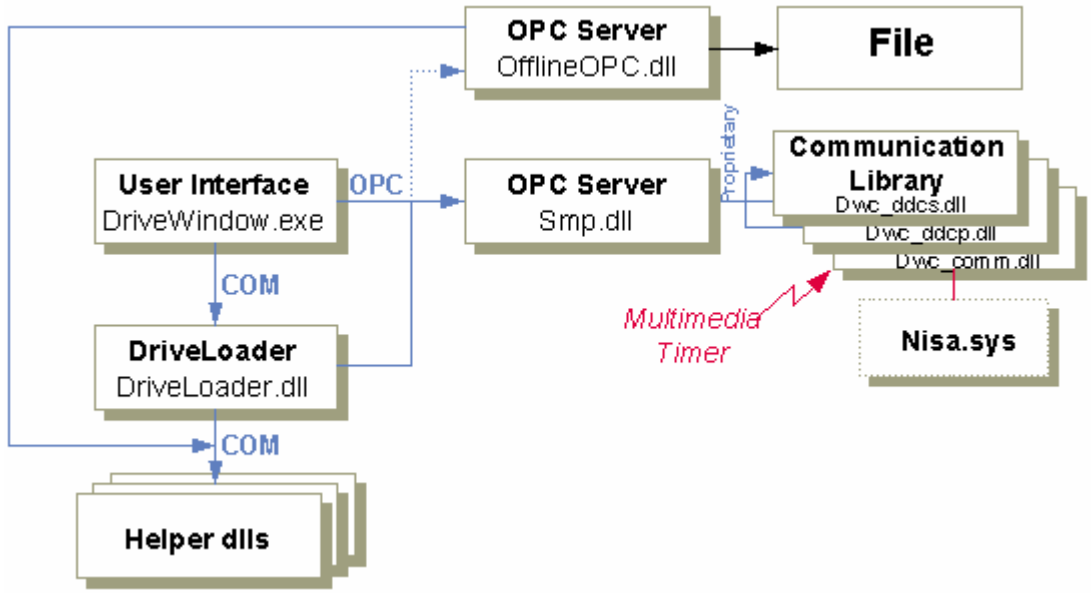
While one user is using a resource, no other user should access to the same resource. Other drives on the drive communication links or other resources on the same drive can be accessed.

There is no internal synchronization of accessing a drive resource. It means that if the configuration allows simultaneous access, the users must agree upon some synchronization policy by themselves.

5. DriveWindow Architecture

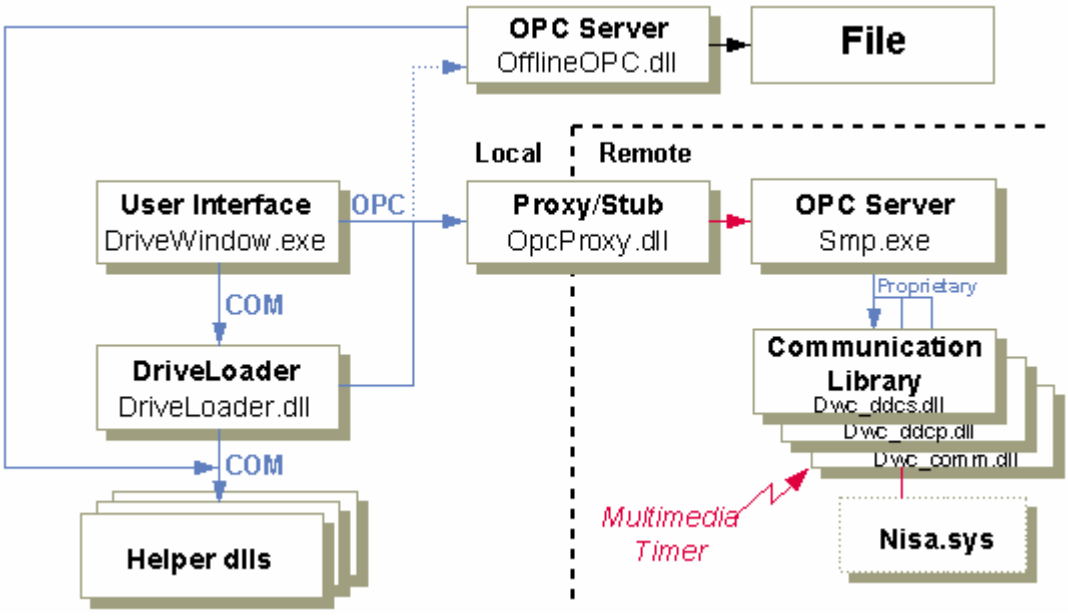
5.1. Local

Architecture of DriveWindow 2 (since version 2.10) when used locally is approximately as follows:



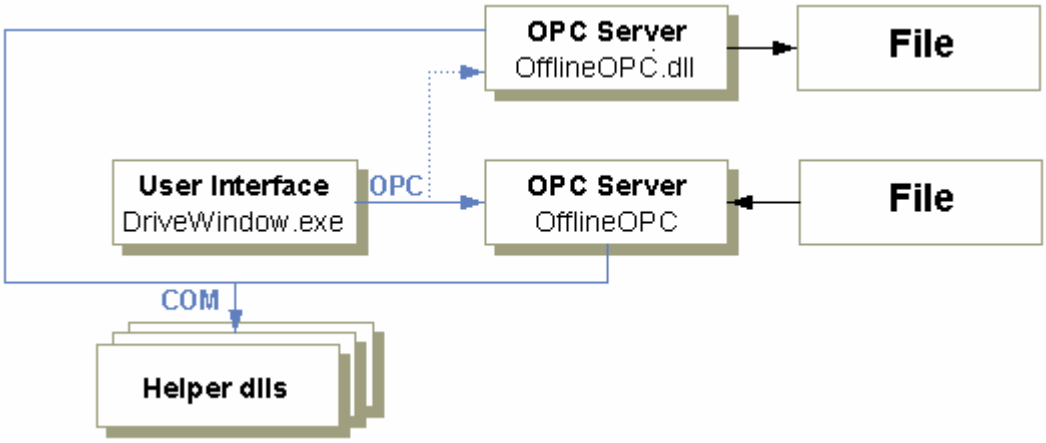
5.2. Remote

Architecture of DriveWindow 2 when used remotely is approximately as follows:



5.3. Off-line

Architecture of DriveWindow 2 when used off-line is approximately as follows:



6. Installation

You need to have local administration rights to do the installation.

A previously installed DriveWindow 2 should be uninstalled before starting a new installation.

6.1. Installation Folder

Default installation folder is <ProgramFilesDir>\DriveWare\DriveWindow.

If you are installing DriveWindow 2 into a computer having an ABB Way NT configuration, we recommend to use the folder C:\LocApps\DriveWare\DriveWindow instead of the default installation folder.

6.2. File and Folder Access Rights

Read Access Right means here that Read and Execute are allowed.

Change Access Right means here that Read, Write, Execute, and Delete are allowed.

Full Control means that all operations (Read, Write, Execute, Delete, Change Permissions, Take Ownership) are allowed.

All folders in the file paths require Read Access Rights.

The following files (and folders in file paths) are installed (unless a newer file already exists) or needed:

File	Required Access Rights
<WINDIR>\DriveLoaderModule.INI	Read
<WINSYSDIR>\ATL.DLL	Read
<WINSYSDIR>\DWC_COMM.DLL	Read
<WINSYSDIR>\DWC_DDCP.DLL	Read
<WINSYSDIR>\DWC_DDCS.DLL	Read
<WINSYSDIR>\MFC42.DLL	Read
<WINSYSDIR>\MFC42LOC.DLL[1)]	Read
<WINSYSDIR>\MSVCRT.DLL	Read
<WINSYSDIR>\OPCPROXY.DLL	Read
<WINSYSDIR>*.DLL	Read
<WINSYSDIR>\DRIVERS\NISA.SYS	Read
<INSTALLDIR>*.*	Read
<INSTALLDIR>\WIN2000*.*	Read
<INSTALLDIR>\WINNT*.*	Read
<INSTALLDIR>\WINXP*.*	Read
<INSTALLDIR>\..\DRIVEOPC\NISADUMP.EXE	Change
<INSTALLDIR>\..\DRIVEOPC *.*	Read
<COMMONFILESDIR>\DRIVEWARE\DRIVEOPC*.*	Read
<COMMONFILESDIR>\DRIVEWARE\OFFLINEOPC*.*	Read
<COMMONFILESDIR>\DRIVEWARE\DWPRINTHTML*.*	Read
<COMMONFILESDIR>\DRIVEWARE\ DRIVELOADER *.*	Read

[1)] Non-English versions only

NISA.SYS is a device driver and its complete installation requires restarting of the computer.

The following files and folders may be needed or are created during run time:

File or Folder	Required Access Rights
<WINDIR>\	Change
<WINDIR>\DWC_DEF.INI	Change
<WINDIR>\CDW.INI	Change
<WINDIR>\DW21.INI	Change
C:\[1)]	Change
<TEMP>\	Change
C:\DWC_*.LOG[1)]	Change

[1)] Only for debugging purposes

6.3. Registry Changes

Installing of DriveWindow adds the following keys (with subkeys) into the registry:

- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Nisa
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\EventLog\System\Nisa
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Pcmcia\DataBase\ABB Industry Oy\Ddcc+
- HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\\Ddcc+1

Since version 2.10, installing of DriveWindow also adds the following keys (with subkeys):

- HKEY_CLASSES_ROOT\.bpg
- HKEY_CLASSES_ROOT\.dwp
- HKEY_CLASSES_ROOT\.dwt
- HKEY_CLASSES_ROOT\.dww
- HKEY_CLASSES_ROOT\.lpg
- HKEY_CLASSES_ROOT\DW2File

Since version 2.10, installing of DriveWindow also adds the following categorisation key, which is not removed by uninstalling:

- HKEY_CLASSES_ROOT\Component Categories\ {63D5F430-CFE4-11d1-B2C8-0060083BA1FB}

Note! Content of HKEY_CLASSES_ROOT is automatically repeated under the key HKEY_LOCAL_MACHINE\SOFTWARE\Classes.

In addition, the following (COM) components register themselves (if installed):

- <WINSYSDIR>\ATL.DLL
- <WINSYSDIR>\MFC42.DLL
- < WINSYSDIR>\OPCPROXY.DLL
- <COMMONFILESDIR>\DRIVEWARE\DRIVELOADER\CONVERSION.DLL
- <COMMONFILESDIR>\DRIVEWARE\DRIVELOADER \CRUSHER.DLL
- <COMMONFILESDIR>\DRIVEWARE\DRIVELOADER \DRIVELOADER.DLL
- <COMMONFILESDIR>\DRIVEWARE\OFFLINEOPC\OFFLINEOPC.DLL
- <COMMONFILESDIR>\DRIVEWARE\DRIVEOPC\SMP.DLL
- <COMMONFILESDIR>\DRIVEWARE\DRIVEOPC\SMP.EXE
- <COMMONFILESDIR>\DRIVEWARE\ DWPRINTHTML \DWPRINTHTML.DLL

Note that SMP.DLL and SMP.EXE register (and unregister) mostly the same keys and values. It means that if either of them is unregistered, the other one must also be either unregistered or re-registered to keep the registry consistent. Note also that in DriveWindow versions prior 2.01 (DriveOPC versions prior 2.02), the installation program did registering of SMP.EXE and SMP.DLL, because registering of either of the components removed the other one from the registry.

7. Local Use

After installation and restarting the computer DriveWindow is ready for local use.

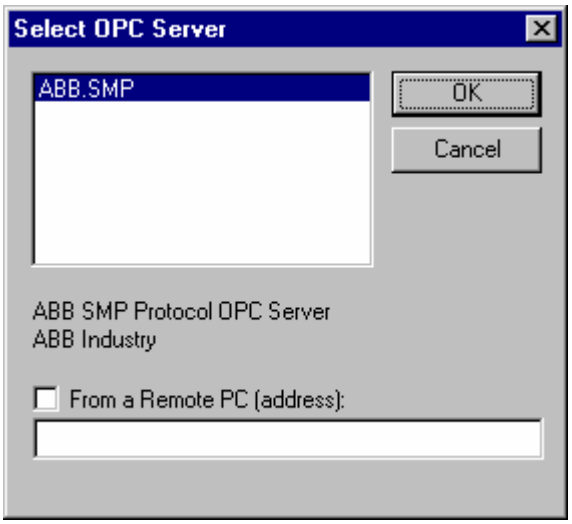
When used locally, DriveWindow requires a NISA-03 DDCS/ISA board or NDPA-02 DDCS/PCMCIA board to be present. With the NDPA-02 board there must be no commercial software handler installed.

When used locally, DriveWindow uses the In-process OPC Server (<COMMONFILESDIR>\DRIVEWARE\DRIVEOPC\SMP.DLL). If more than one instance of DriveWindow (or some other application using the In-process OPC Server) is started, they all have their own copy of it. The Communication Library uses a global semaphore, however, which prevents all but one application to communicate with the Drives. All others get an error. DriveWindow does not display the error, but it displays no drives instead.

Instructions for installing NISA-03 DDCS/ISA and NDPA-02 DDCS/PCMCIA boards are not given here, because they are documented elsewhere.

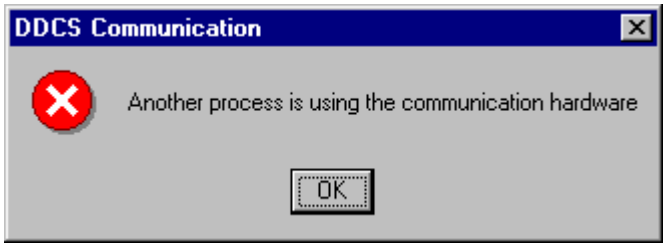
If device addresses are other than default and registry changes have to be made (NISAREG), they have to be made after DriveWindow installation.

If installation is done properly, DriveWindow lists ABB.SMP in the Select OPC Server dialog box shown when it starts. Clicking OK starts DriveWindow locally.



If NISA-03 DDCS/ISA or NDPA-02 DDCS/PCMCIA is not installed properly, Communication Library displays a message box telling that it did not find any communication hardware.

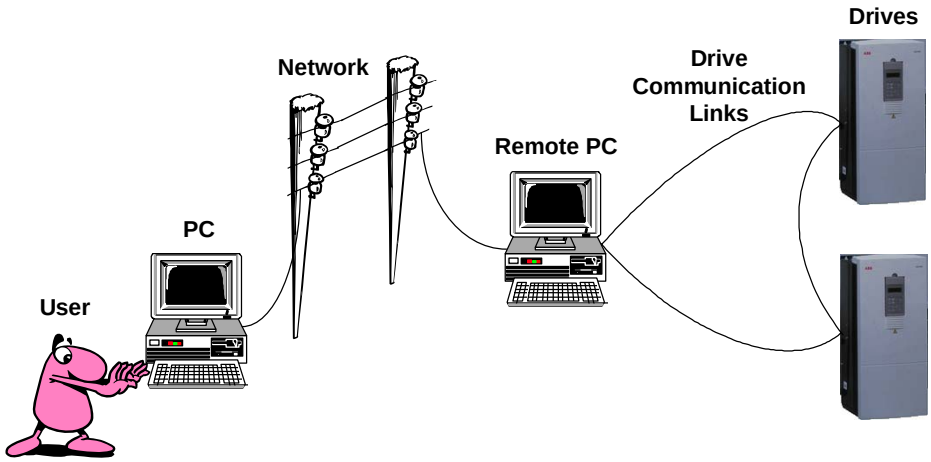
If another application program is currently using the Communication library, Communication Library displays a message box telling that another process is using the communication hardware (since DriveWindow 2.01).



Note! All messages from the Communication Library are inhibited, if <WINDIR>\DWC_DEF.INI contains Remote=1 in the [OPC] section. The INI-file is not included in the installation but made by the Communication Library during run time.

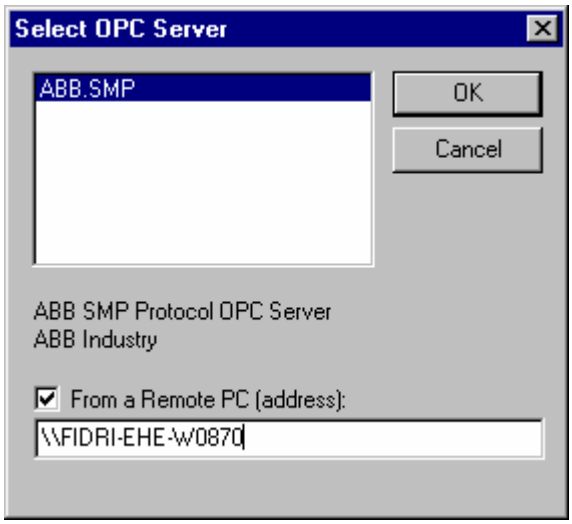
8. Remote Use

In addition of using DriveWindow locally (i.e., the drive communication links are connected to the PC operated by the user), it can also be used remotely (i.e., the PC operated by the user is connected by a network to the PC containing the drive communication links).



Remote Use

If installation and configuring are done properly at both ends, the remote end can be contacted by checking From a Remote PC (address) in the Select OPC Server dialog box shown when DriveWindow starts. The name or IP address of the remote end computer has to be entered into the field below it. Clicking OK connects DriveWindow to the OPC Server at the remote end.



When used remotely, DriveWindow uses the Local OPC Server (<COMMONFILESDIR>\DRIVEWARE\DRIVEOPC\SMP.EXE) at the remote end. It is possible to configure the remote end to use the In-process OPC Server running under Microsoft DLLHOST.EXE, too.

If the remote end is configured as it should be, a single Server is shared among simultaneous users. If configuring allows more than one instance of the server, the Communication Library handles the situation. It has a global semaphore, which prevents all but one application to communicate with the Drives. All others get an error. DriveWindow does not display the error, but it displays no drives instead.

DriveWindow 2 uses fixed names when creating groups in the OPC Server and gets an error in case any of the groups already exist. DriveWindow 2 considers this error to mean that another instance of DriveWindow 2 is already using the OPC Server and tells about it to the user. The fixed groups are created during connecting to the server and connection is refused in case of error.

Configuring a computer to serve as remote end does not prevent DriveWindow to be used locally as well. It runs in a different window station, however. It requires special settings (not explained in this document) at the remote end, if the remote end is to be used locally sharing the same Local OPC Server. In any case, the Communication Library at the remote end does not show any message boxes when DriveWindow is used locally at the remote end.

8.1. Installing for Remote Use

DriveWindow 2 has to be installed at client end. At remote end you can either install DriveWindow 2 or DriveOPC.

At the client end there is no need for communication boards if the client end uses DriveWindow only remotely.

At the remote end DriveWindow or some other OPC client program has to be started locally after the installation to check the proper installation of the drive communication boards.

The minimum requirement of using DriveWindow remotely is to edit at the remote end the file <WINDIR>\DWC_DEF.INI (created by the Communication Library at time DriveWindow was started locally). You have to add section [OPC] with setting Remote=1 into it. It inhibits all messages from the Communication Library.

Note! Message boxes, which the Communication Library may show in some error conditions, hang up the Remote OPC Server, because the messages go to a non-interactive window station, where nobody can see them and it is not possible to click the OK button. Only if the OPC Server is launched as interactive user, the message boxes are shown on the interactive window station (if there is an interactive user logged on), but this is usually configuration used only during debugging.

Unless no other configuration is made, the remote end can usually be used remotely by administrators.

8.2. Configuring the Remote End

The remote end configuration requires local administration privileges and is done by using the User Manager and DCOMCNFG.EXE Windows NT utility. DCOMCNFG is usually not found in the start menu, but must be started by selecting Run from the Start menu.

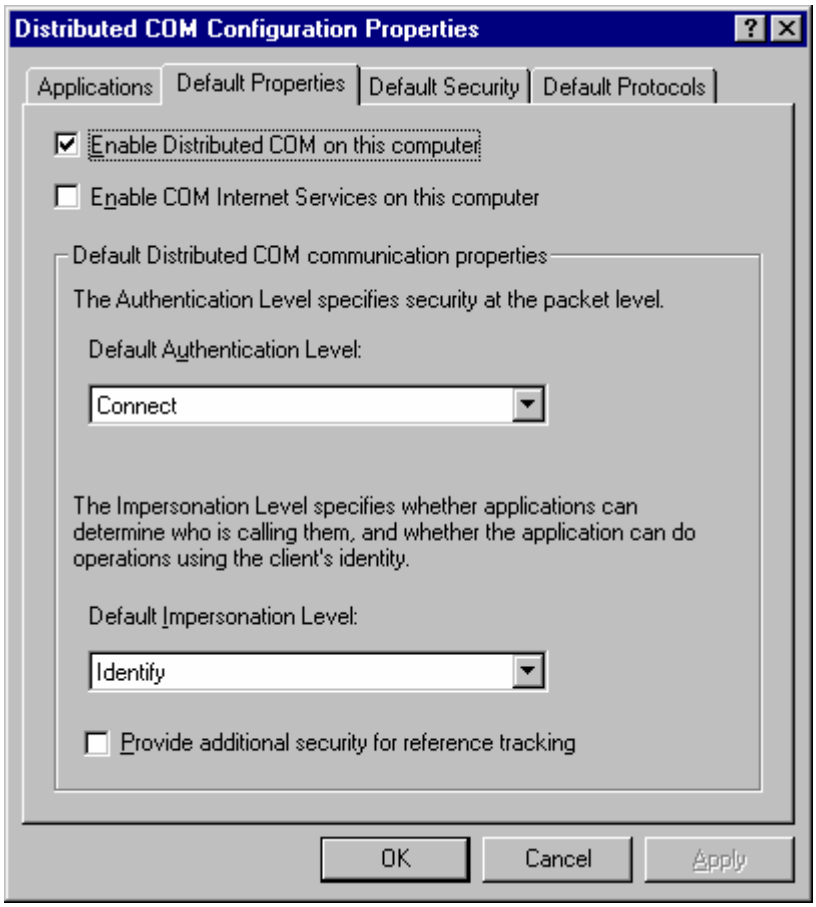
It is possible to do the configuring in several ways and there can be lot of different security requirements in different cases. We present here just an example as a guideline, which we hope to cover the most typical cases.

In the example we will configure the remote end so that all users, who have access to the remote end computer through the intranet, can use the OPC Server at the remote end. It means that in addition to the users (everyone) of the trusted domains, also guests from other domains are allowed to access the remote end computer.

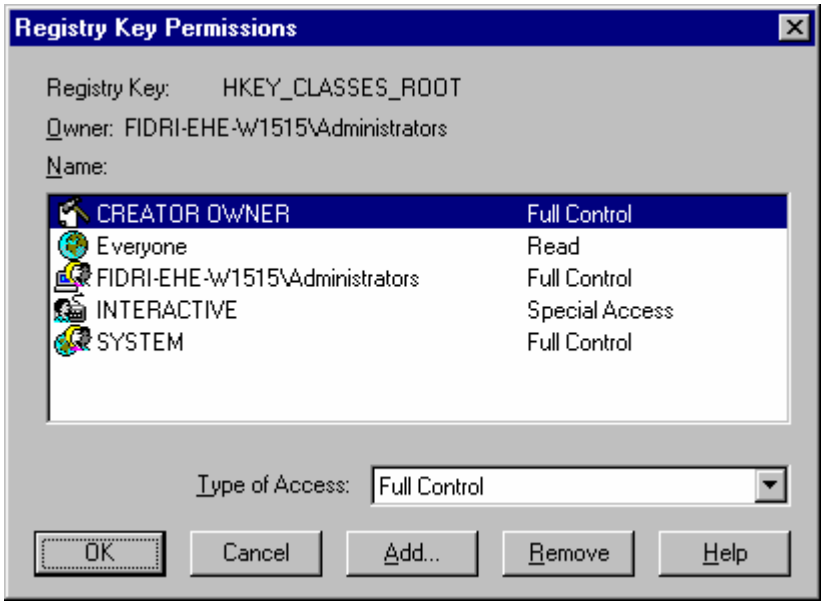
Although not absolutely necessary, we recommend that you restart the computer after you have done the configuring.

8.2.1. Some Assumptions

In the DCOMCNFG, we assume that the list of Default Access Permissions is empty (actually means that system and interactive user has the access). We also assume that Default Launch Permissions list consists of the local administrators, the interactive user, and the system all having Allow Launch permission, and the Default Properties settings are the following (or you at least know the Default Authentication Level setting):



Although the following settings are not much concern in configuring the remote end as long as you are able to change registry settings, we assume that the Default Configuration Permissions are:

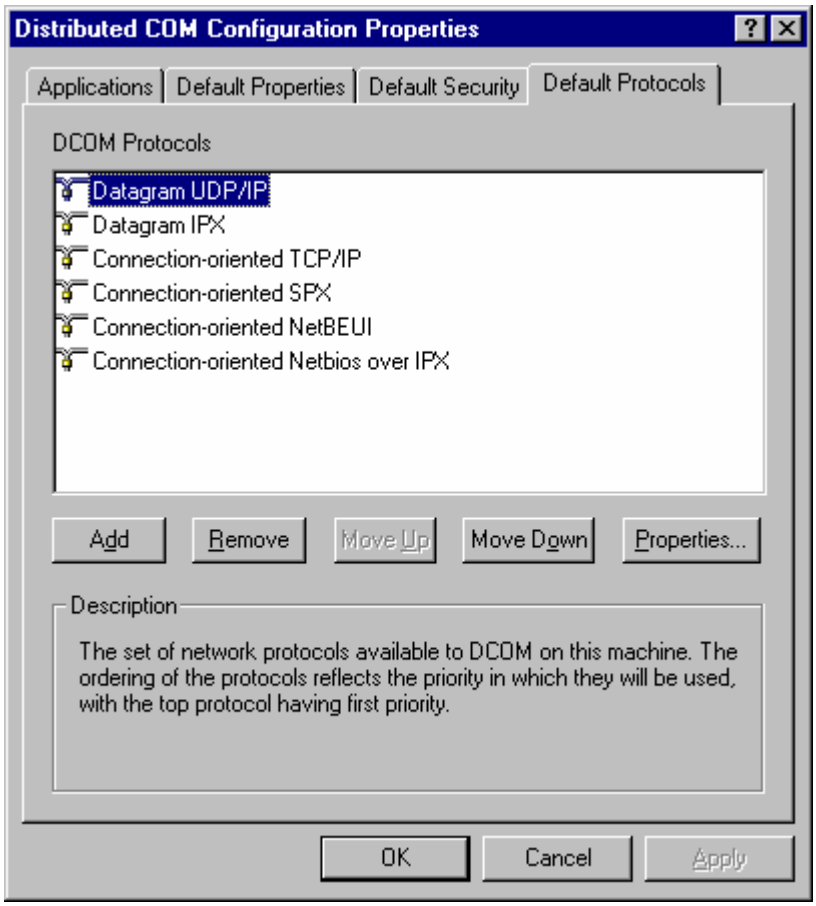


Read Access means that Query Value, Enumerate Subkeys, Notify, and Read Control are allowed.

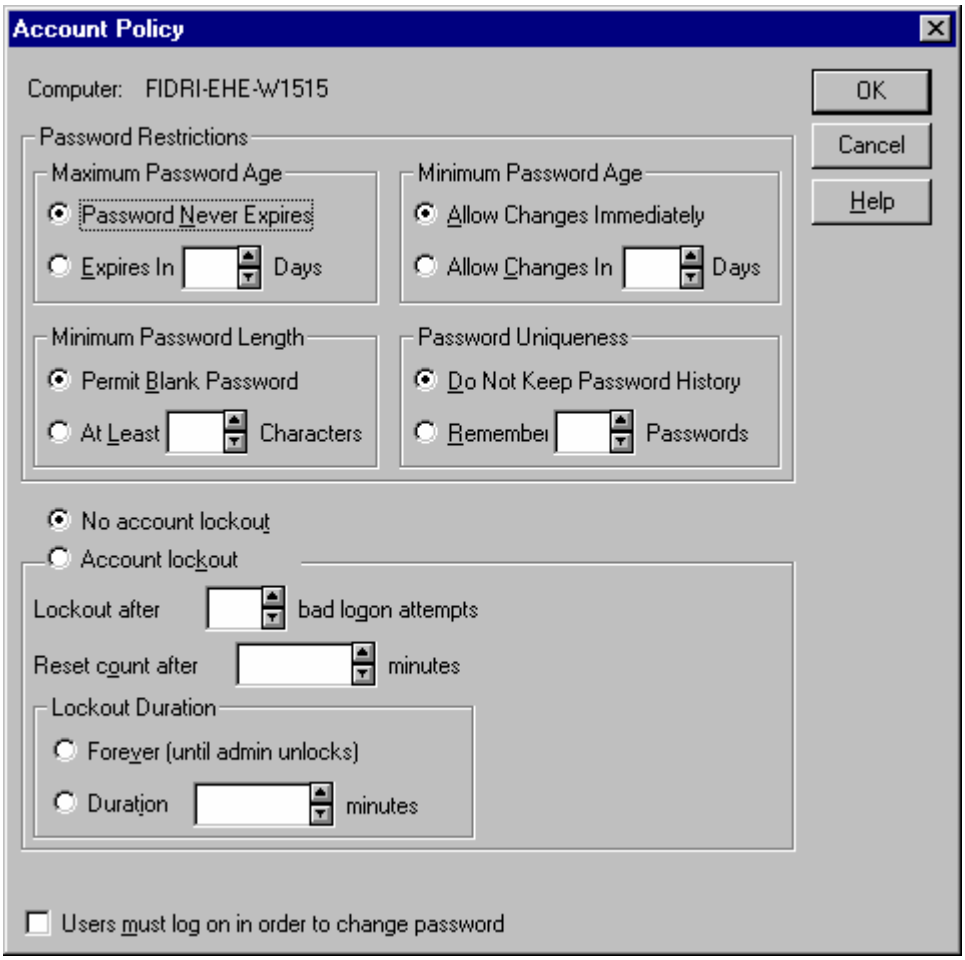
Special Access means that Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Delete, and Read Control are allowed.

Full Control means that all operations (Query Value, Set Value, Create Subkey, Enumerate Subkeys, Notify, Create Link, Delete, Write DAC, Write Owner, Read Control) are allowed.

We assume that Datagram UDP/IP is at the highest priority of the Default Configuration Protocols:



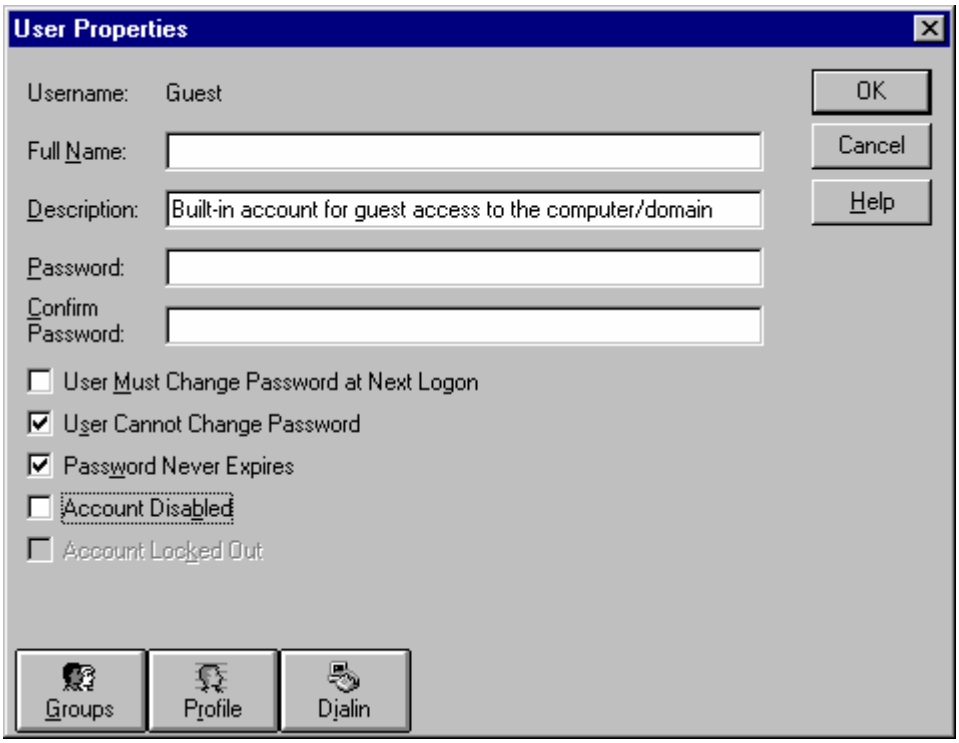
We also assume the following account policy. Especially blank passwords must be allowed. Changes can be made by using User Manager.



8.2.2. Users

You have to decide, who are the users that are allowed to launch (start SMP.EXE or DLLHOST.EXE) and access the OPC Server at the remote end. Although in general it is possible to have different launching and accessing users, remote use of DriveWindow requires that they are the same.

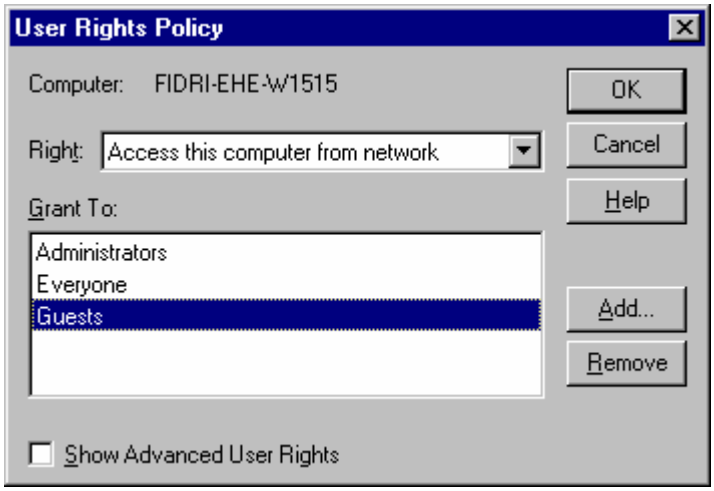
If you are going to allow guests to access to the remote end, you must enable the Guest account by using the user manager. Also, you must clear the password.



8.2.3. Right to Access the Remote Computer from Network

Any user, who should be allowed to use the remote end computer from a client computer, must have proper access right to do that. The right can be set by the User Manager program of the remote computer, for example. You select User Rights Policy, the right Access this computer from network, and add or remove users or group of users, which are granted to have that right.

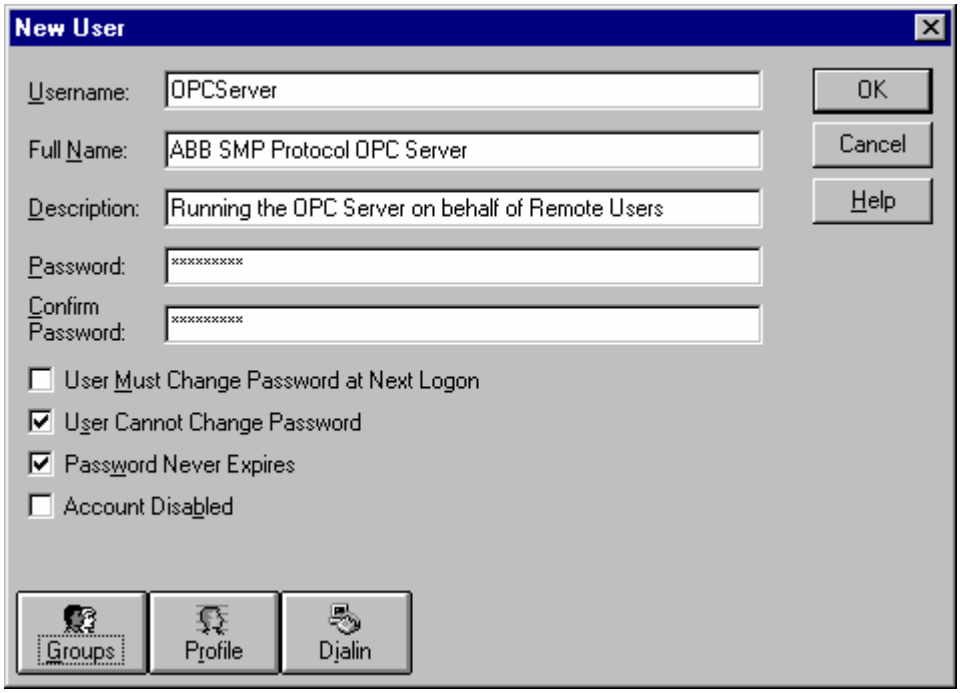
To grant access to guests and everyone, for example, the groups Everyone and Guests have to be in the Grant To list.



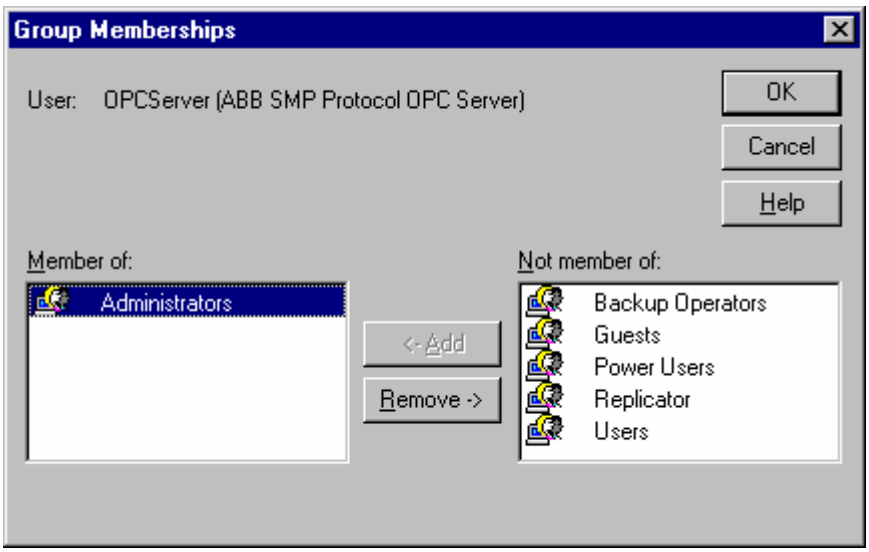
8.2.4. Adding a Special Account for the Remote OPC Server

We recommend that a single window station is shared with all simultaneous clients. Therefore, you need to specify a user account to be used in launching. This user account can be an already existing one with enough privileges (your account, for example). However, it is more clear to add a special account solely for launching the OPC Server at the remote end computer.

The account is added by using the User Manager program.

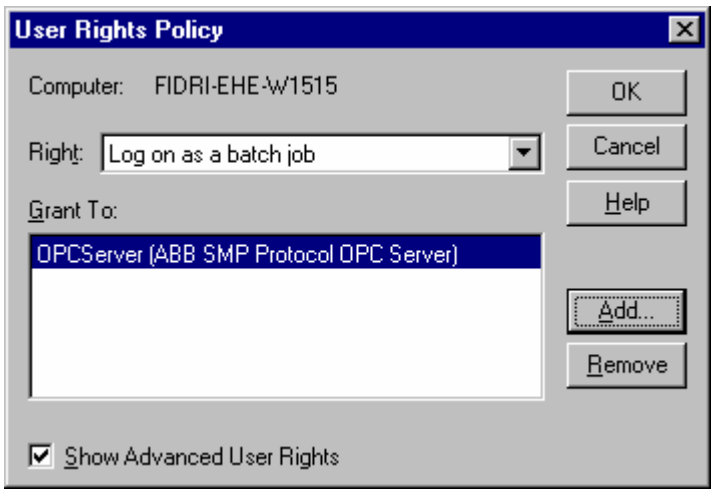


The easiest way to get the OPCServer running is to give the OPCServer privileges of the Administrators group.



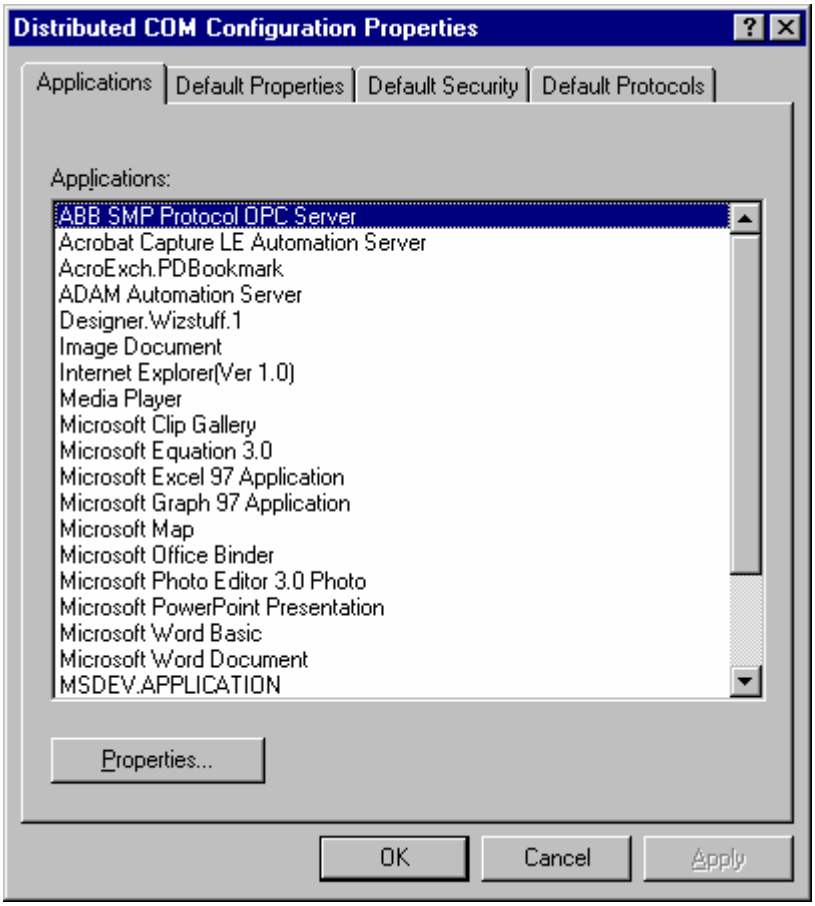
OPCSever account must be able to run DriveWindow. Unless OPCServer belongs to a group that has proper file and folder access rights (administrators, for example), you may need to edit permissions of all files and folders required by DriveWindow. Editing can be done by selecting Properties in the NT Explorer for the file(s) and/or folder(s) selected, and from the Security tab, selecting Permissions.

The account must also have the right to log on as a batch job. Although it is not necessary to grant it separately, because it is done automatically by DCOMCONF when needed, you can do it by using the User Manager, too. You grant it by selecting User Rights from the Policies menu, setting Show Advanced User Rights, selecting Log on as batch job, and finally adding the OPCServer.



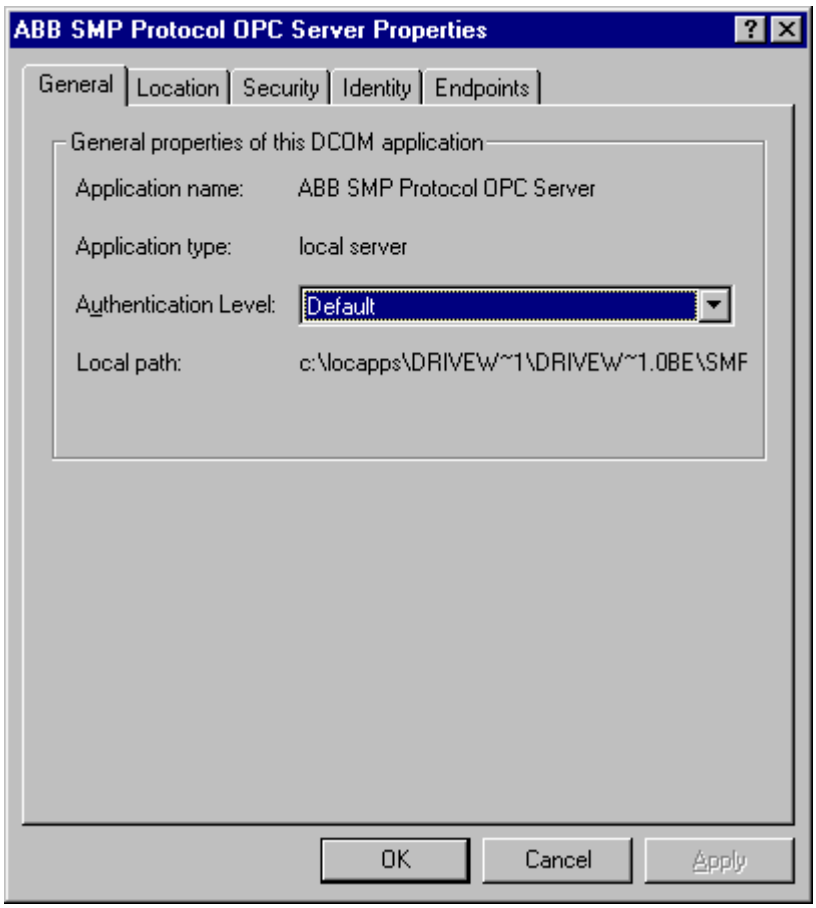
8.2.5. Configuring the Remote End OPC Server

To configure the OPC Server, start DCOMCNFG.EXE on the remote end computer. In the Applications tab, browse ABB SMP Protocol OPC Server, select it, and click Properties button.



8.2.5.1. Authentication Level

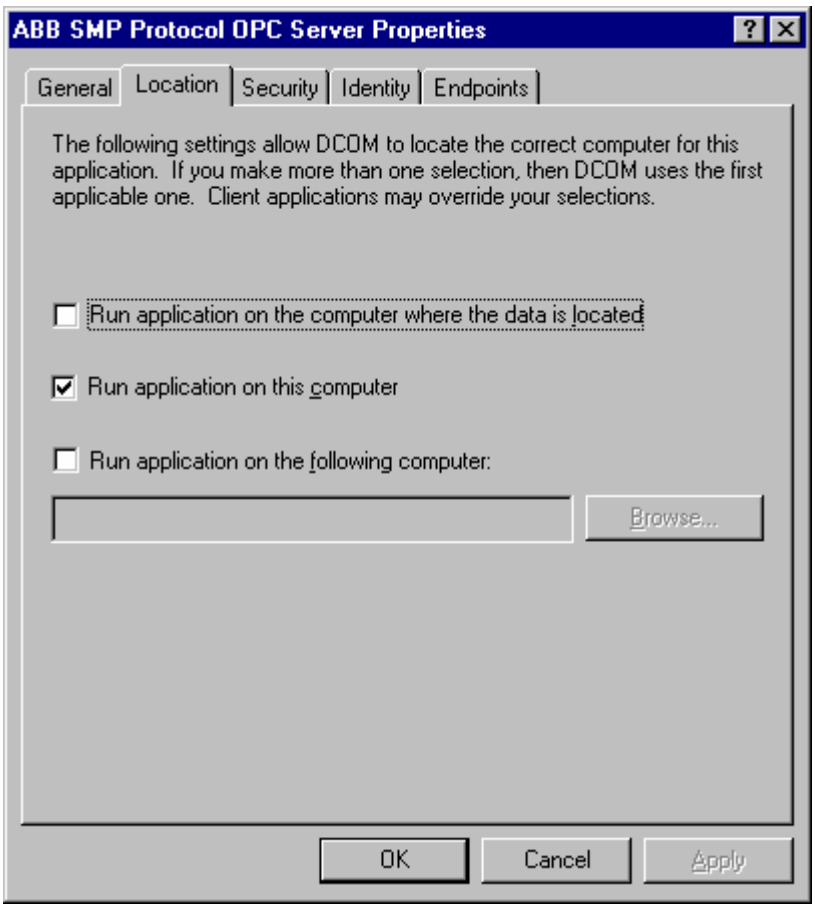
Usually there is no need to use other than the Default authentication level for the OPC Server at the remote end computer.



Note! Datagram transports such as UDP default to packet-level authentication if a lower level authentication level is requested, because datagram transports do not maintain a virtual connection between the client end and the remote end. Therefore, each transmitted packet has to be authenticated individually.

8.2.5.2. Location

Run application on this computer must be checked for the OPC Server at the remote end computer.

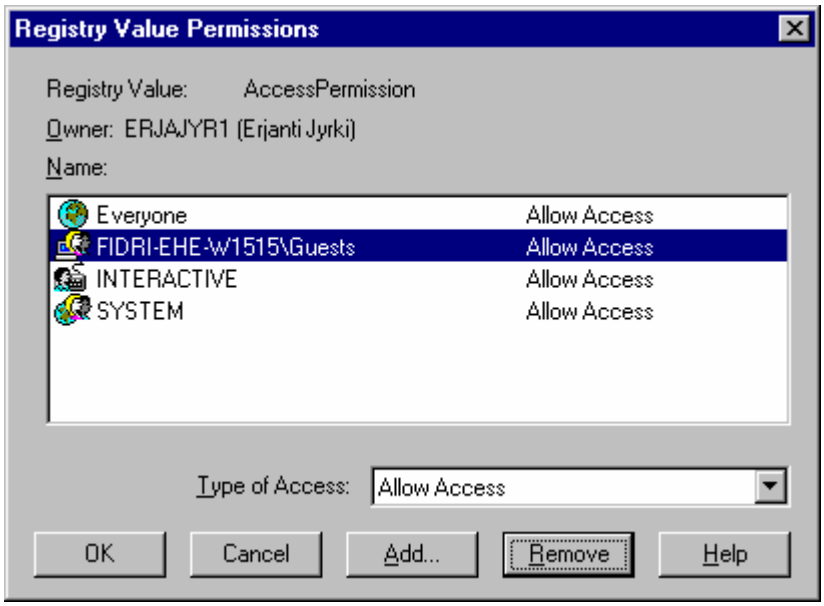


8.2.5.3. Endpoints

Default system protocols are usually enough for the OPC Server at the remote end computer.

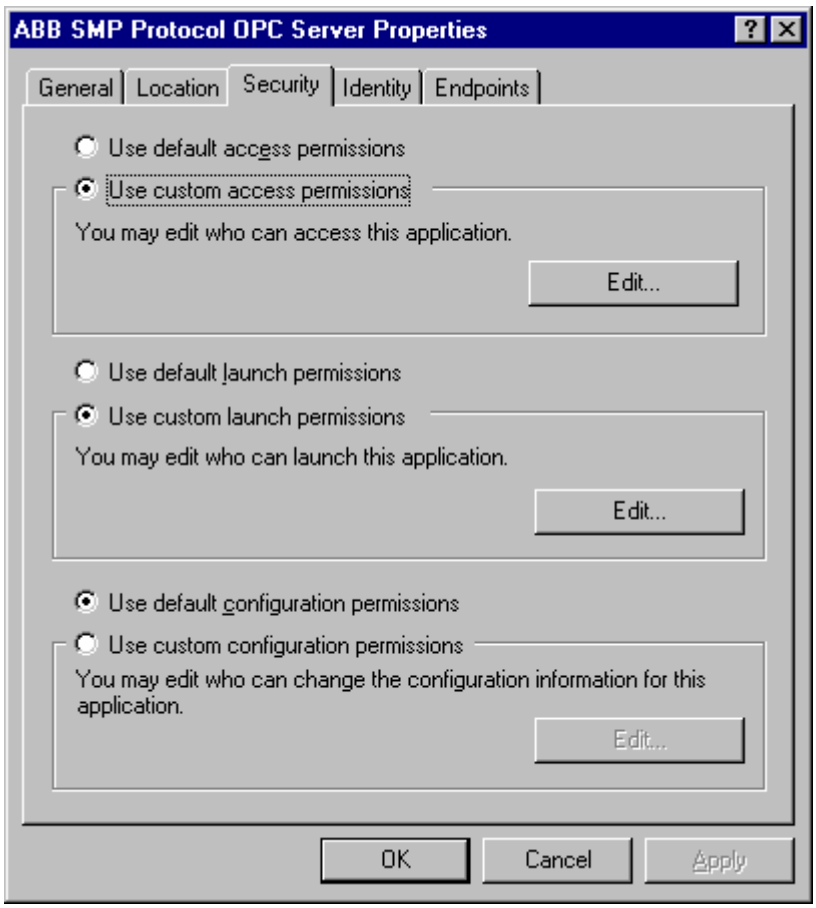
8.2.5.4. Access Permissions

By editing the access permissions of OPC Server at the remote end computer, you control, who can access OPC Server. For example, if guests and everyone should be able to access the computer, you must allow everyone and guests to launch OPC Server.



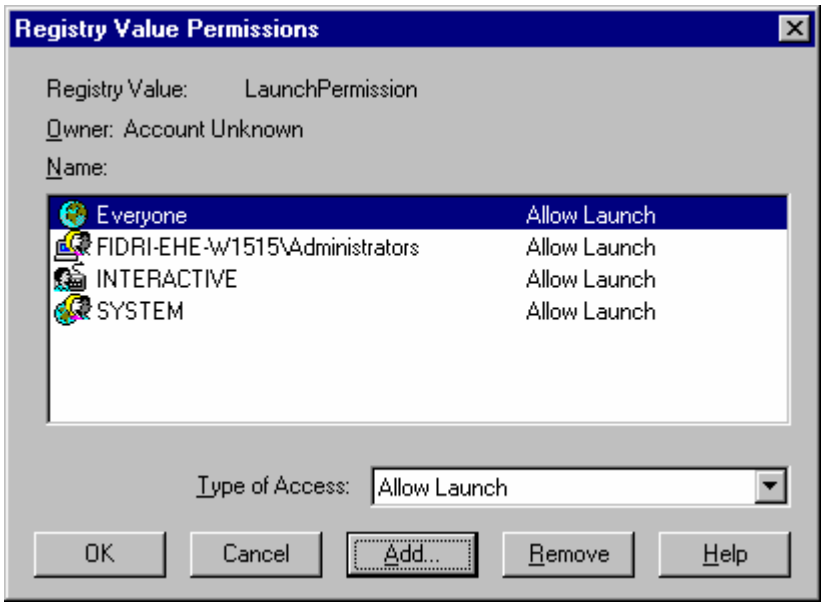
8.2.5.5. Configuration Permissions

Our experiments show that you should select default configuration permissions for OPC Server at the remote end computer.



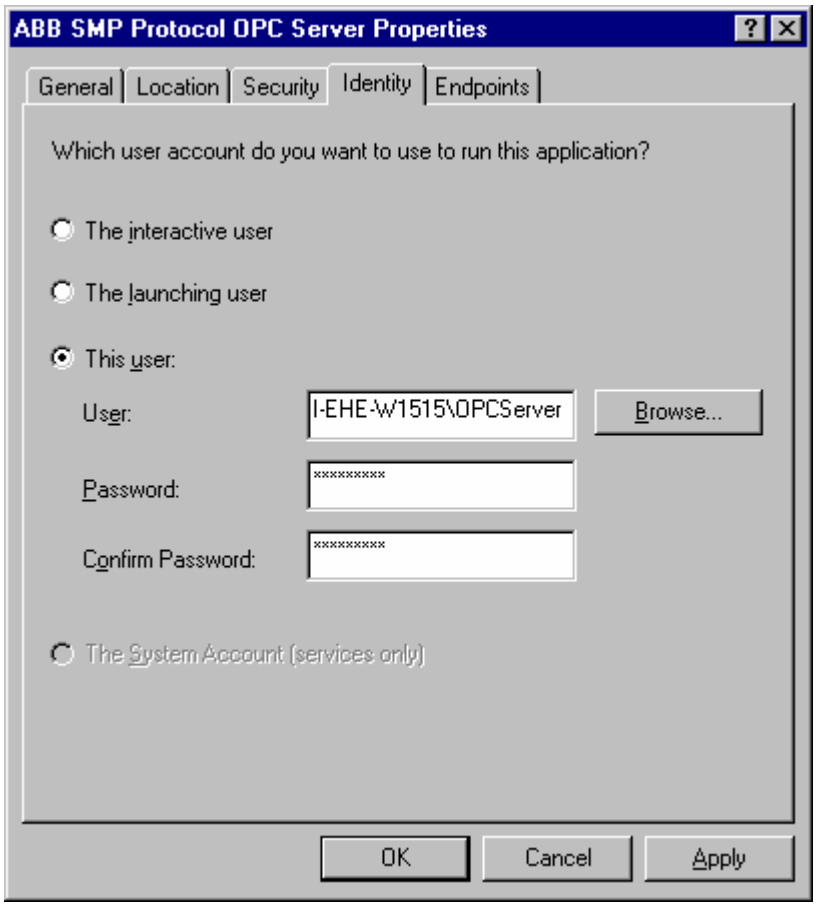
8.2.5.6. Launch Permissions

By editing the launch permissions of the OPC Server at the remote end computer, you control, who can launch the OPC Server. For example, if guests and everyone should be able to access the computer, you must allow everyone to launch the OPC Server (guests seem to be included in everyone here).



8.2.5.7. Launching Identity

The remote end OPC Server is configured to use the account of the OPCServer (or some other user, if you decided otherwise). You must know the password of the user in order to be able to set the launching identity to be a specific user.

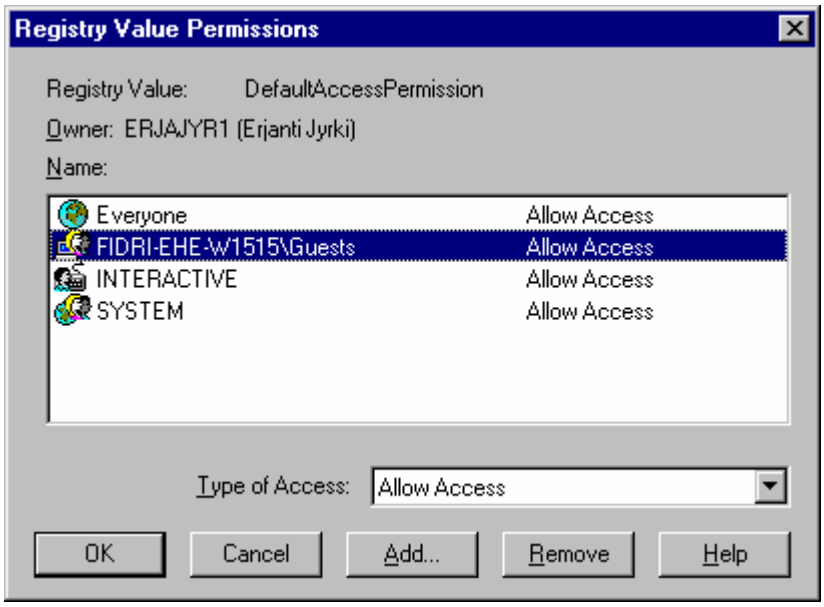


Note! When you set the OPC Server to use a specific user account, DCOMCNFG also grants the account the privilege to log on as a batch job.

Interactive user can be used for debugging purposes only. The launching user should be avoided, because (by design) Windows NT does not allow OPC Server to access network at all. Thus call-backs (monitoring, for example) do not work.

8.2.5.8. Changing the Default Access Permissions

Our experiments show that sometimes access permissions of the OPC Server must be set into the defaults, because the custom access permissions seem not to have any effect. In addition to the users (guests and everyone, for example), you have to allow the system and the interactive user to access components at the remote end.



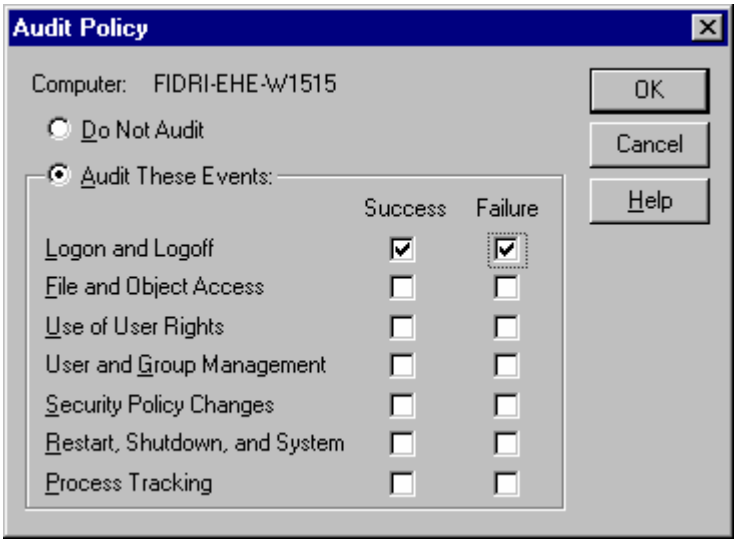
8.3. Configuring the Client End

Current version of DriveWindow needs no configuration to be done to be able to connect and use a remote OPC Server.

8.4. Auditing the Remote End

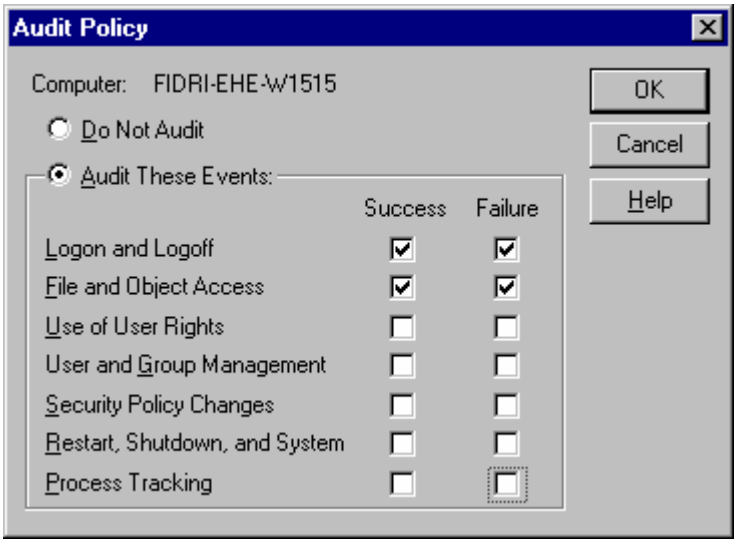
8.4.1. Configuring for Audit

If you want to log use of the remote end computer, you should enable auditing in the User Manager program. All logons and logoffs, interactive or from network, can be audited, whether successful or not, for example, by selecting:

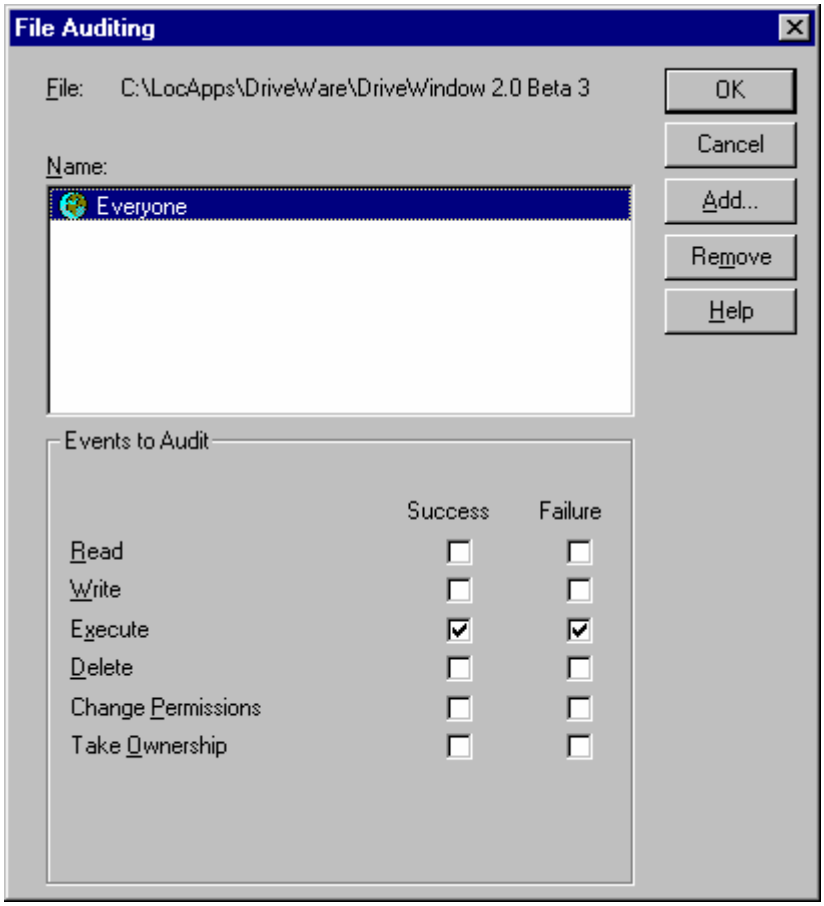


Note! Security logs are limited in size, so select auditing events wisely. The maximum size of the security log is defined in Event Viewer.

You have also the possibility to audit use of selected files and other objects if you checked File and Object Access in the User Manger Audit Policy.

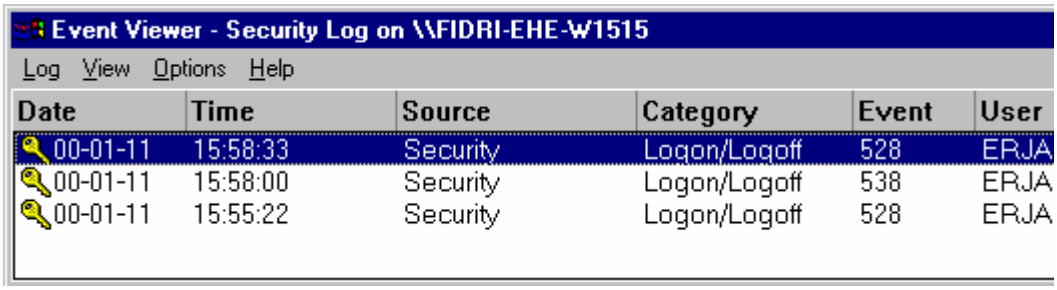


To audit the use of SMP.EXE, for example, browse and select it in the NT Explorer, use right mouse button to show its properties, and in the Security tab click Auditing. Now you can add users or group of users to audit (everyone, for example), and type of access you want to audit (execution, for example).

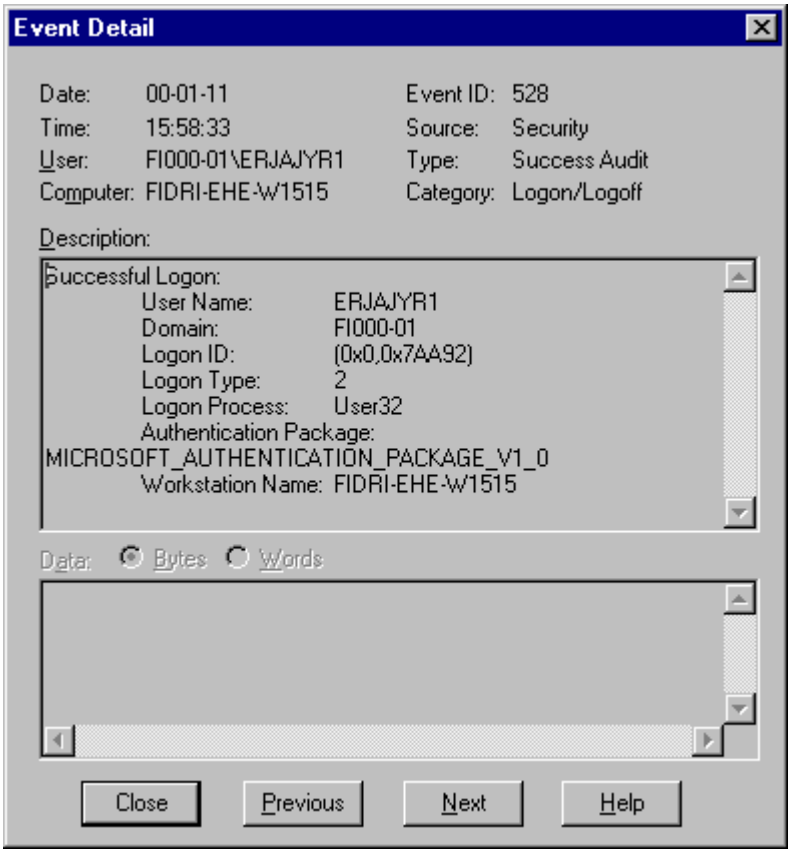


8.4.1.1. Viewing Audit Logs

The log can be viewed by selecting Security Log in the Event Viewer program.



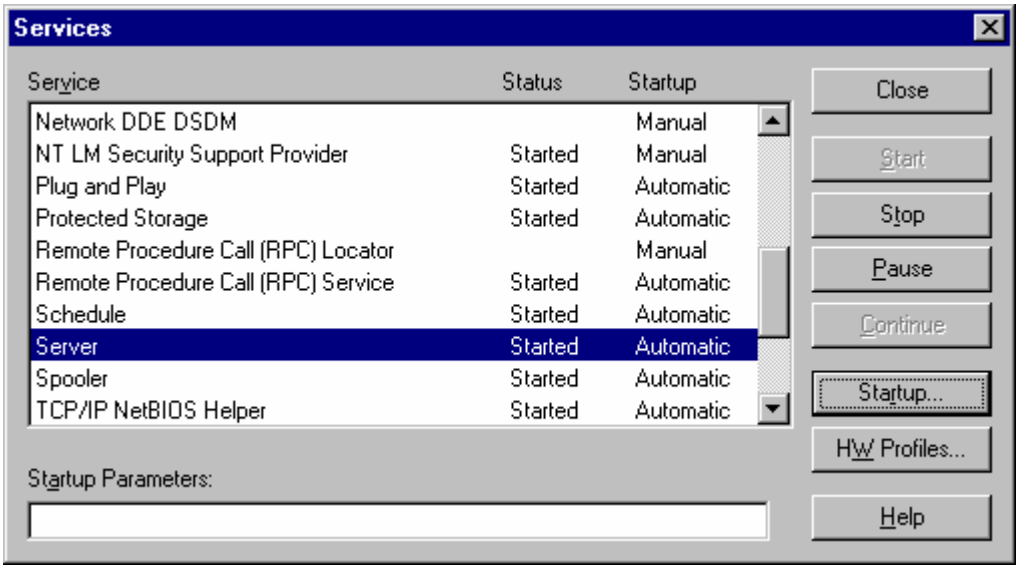
Details of a single event can be viewed as well.



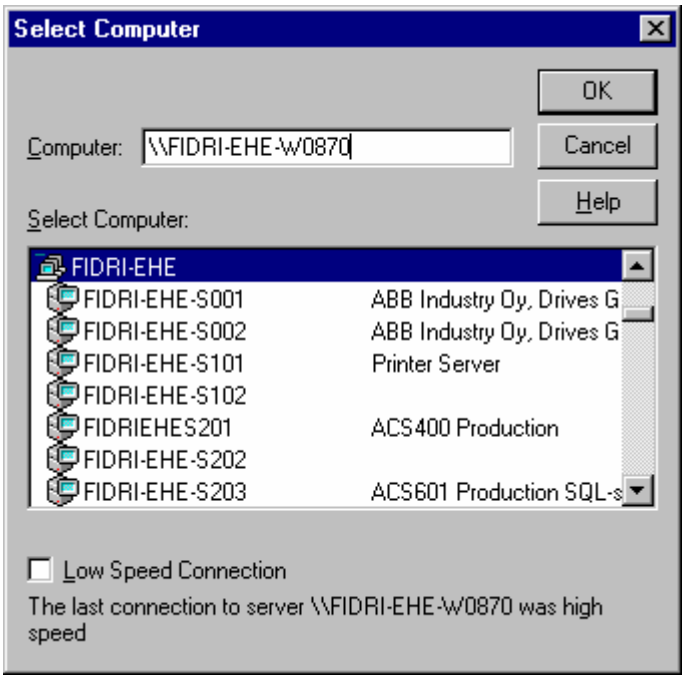
8.4.1.2. Viewing Audit Logs Remotely

If you are administrator at both ends, you can view the remote end event log from the client end as well. The prerequisite is, however, that Server service has been started (manually or automatically) at the remote end.

You can start the Server service and control, how it is to be started, by selecting Services from the Control Panel at the remote end.



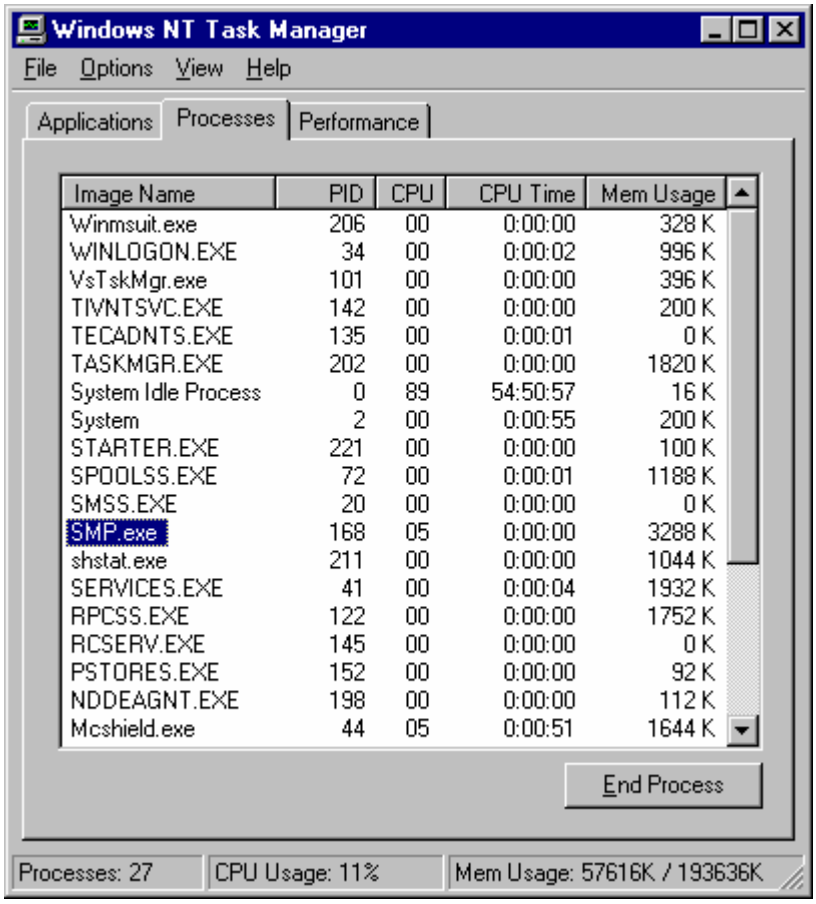
At the client end, select Select Computer from the Log menu of the Event Viewer and enter the name or the address of the remote end computer.



8.4.1.3. Instances of SMP.EXE at the Remote End

If you want to know, how many instances of SMP.EXE are currently running on the remote end computer, start the Task Manager (click right mouse button on the taskbar and select Task Manager).

In the Task Manager, select the Processes Tab and click the title Image Name twice to get the listed images into alphabetical order. Scroll for SMP.EXE and count the instances. If the remote end is configured properly, there should be most one instance shown.



Note! If there is more than one instance of SMP.EXE, only one of them is actually connected to the Drives because of internal synchronisation within the Communication Libraries (which does not work properly yet across window stations).

Terminating SMP.EXE (because it hangedd up, for example) by using the Task Manager is not usually possible. You will get an error message. To terminate it, you have to restart the remote end computer.

8.5. Simultaneous Local and Remote Use

If local user at the remote end connects to the drives locally, either she or all the remote users see no drives.

8.5.1. Denying Local Use at Remote End

It is not possible to prevent using OPC Server locally at the remote end, unless you also deny remote use for those, who are using the remote end locally. However, you can deny access to applications running at the remote end, which use OPC Server.

8.5.2. Forcing Remote Use instead of Local Use at the Remote End

Although it is possible to configure a computer always to use a pre-defined remote computer instead of local use, such a computer cannot be used remotely. The reason is that also remote calls to such a computer are then directed to the another, pre-defined remote computer.

Thus it is not possible to force remote use instead of local use at the remote end.

8.6. Pre-defined Remote Use instead of Local Use

It is possible to configure the client end computer to connect to a pre-defined remote end computer when the user tries to connect locally. Such a computer can never be the remote end and it does not need to have drive communication hardware installed.

To do so, you use DCOMCNFG.EXE at the client end and, instead of running the OPC Server on this computer, you specify the remote end computer (name or address), on which the OPC Server is to be run. In addition you have to ...(will be added later).

8.7. Using In-Process Server at the Remote End

It is possible to configure the remote end computer to use the in-process OPC server (SMP.DLL) instead of the local server (SMP.EXE). In this case, the in-process server is configured to run under DLLHOST.EXE, which is a Microsoft made program.

There is no advantage of using the in-process server remotely. However, for maintenance reason, we may in the future stop supporting the local server (SMP.EXE) and use the in-process server only - both locally and remotely.

To use the in-process OPC Server instead of the local server at the remote end, you have to do the following ...(will be added later).

9. External References

In addition to a normal operating system installation the DriveWindow program does not require any other programs or modules to be present. All modules required are included in the DriveWindow installation.

10. Other Features

10.1. Performance

Drive communication link speed limits performance the drive handling functions.

PC hardware configuration and the internal processing done within DriveWindow limit performance of functions that need excessive processing power or huge amount of data.

When remotely connected, the network limits DriveWindow response to user actions.

10.2. Usability, Recovery, Safety and Protection

DriveWindow does not include specific recovery, safety, or protection. Recovery, safety, and protection are handled by the operating system and depend on its settings.

10.3. Maintenance

As being an application based on COM modules, upgrading to a newer revision can even be done module by module.

10.4. Portability and Compatibility

DriveWindow runs under Windows NT 4.0 SP3 (or newer), Windows 2000, or Windows XP operating system in a x86 PC.