

DCOM Einstellungen zur rechnerübergreifenden Kommunikation zwischen OPC Server und OPC Client

1. Einleitung

Für die rechnerübergreifende Kommunikation zwischen OPC Client und OPC Server wird bei OPC DA das Dienstprogramm „dcomcnfg“ verwendet.

Bei diesem Dienstprogramm gibt es abhängig vom benutzten Betriebssystem (Windows 98 / 2000 / XP / XP SP2) diverse Unterschiede in Aussehen und Verhalten. Dieses Dokument bezieht sich auf Windows 2000 und Windows XP SP2. Bei Aspekten, die nur für Windows XP SP2 relevant sind wird im Text darauf hingewiesen.

Bei DCOM sind nur authentifizierte Zugriffe zwischen den Rechnern möglich. Wir empfehlen, die Rechner in derselben Domäne anzumelden und auf allen Rechnern eine Benutzergruppe (z.B. „OPC-User“) für die OPC-Kommunikation festzulegen.



Hinweis:

„dcomcnfg“ greift sehr tief in das Betriebssystem ein. Eine Fehlkonfiguration kann dazu führen, dass das Betriebssystem nicht mehr (stabil) läuft. Die Einstellungen, die hier vorgenommen werden setzen die Sicherheit Ihres Systems herab.

Eine Alternative bietet das Tool „[Softing OPC Tunnel](#)“. Hierbei sind keine DCOM-Einstellungen notwendig. Das letzte Kapitel stellt dieses Tool kurz vor.



Hinweis:

Unter Umständen gibt „dcomcnfg“ DCOM-Konfigurationswarnungen heraus. Dabei werden Sie gefragt, ob Sie automatisch Unstimmigkeiten in der DCOM-Konfiguration beseitigen möchten. Für die hier beschriebenen Einstellungen ist diese Beseitigung nicht notwendig.

2. DCOM-Einstellungen für systemweite Sicherheitsparameter

Die nachfolgenden Einstellungen sind auf dem Client-Rechner, und dem Server-Rechner durchzuführen.

2.1. „dcomcnfg“ starten

- Login mit Administrator-Rechten
- Windows-Startmenü öffnen
- „Ausführen...“ auswählen
- „dcomcnfg“ eingeben
- „OK“-Taste drücken

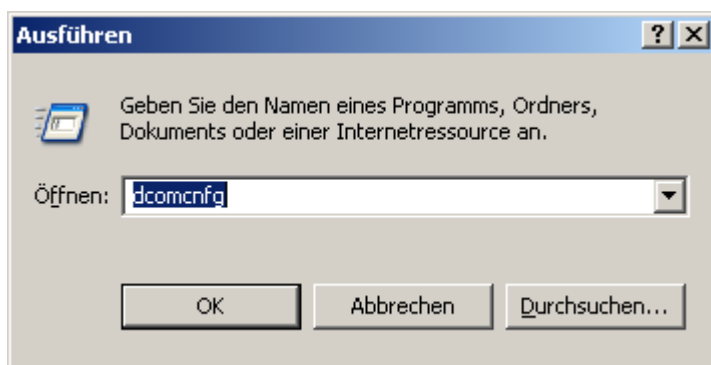


Abbildung 1: Der "Ausführen"-Dialog von Microsoft Windows

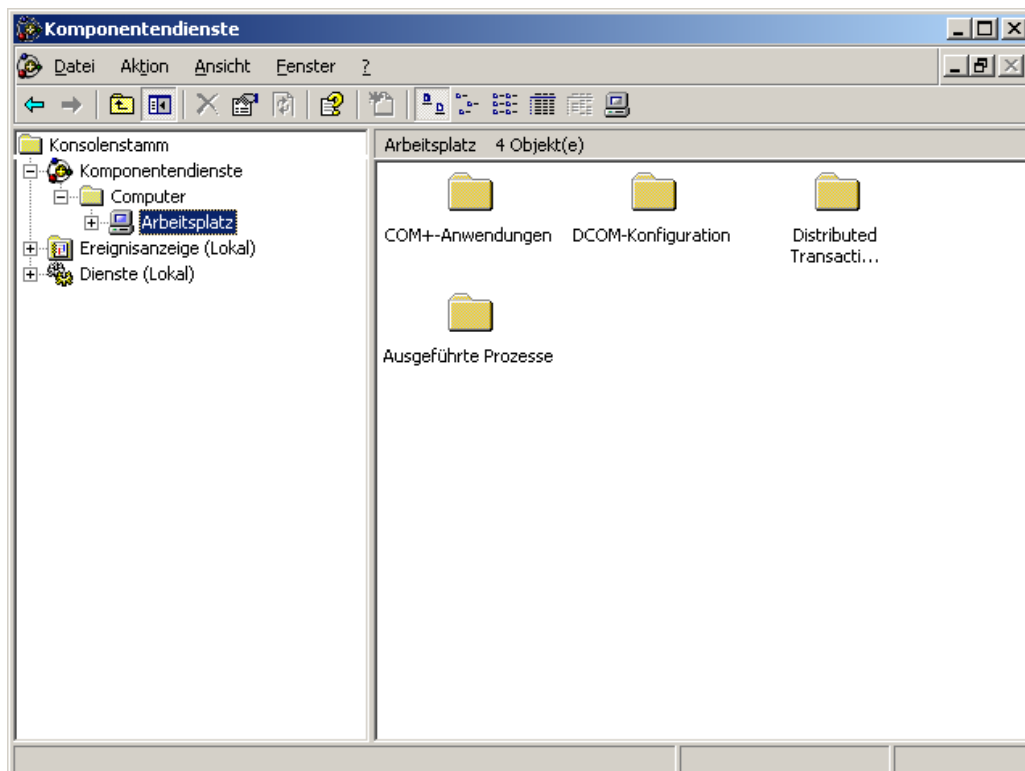


Abbildung 2: Startseite von "dcomcnfg"

2.2. Öffnen des Dialogs „Eigenschaften von Arbeitsplatz“

- „Konsolenstamm / Komponentendienste / Computer / Arbeitsplatz“ in Baumansicht auswählen
- Kontextmenü öffnen (rechte Maustaste) → Eigenschaften

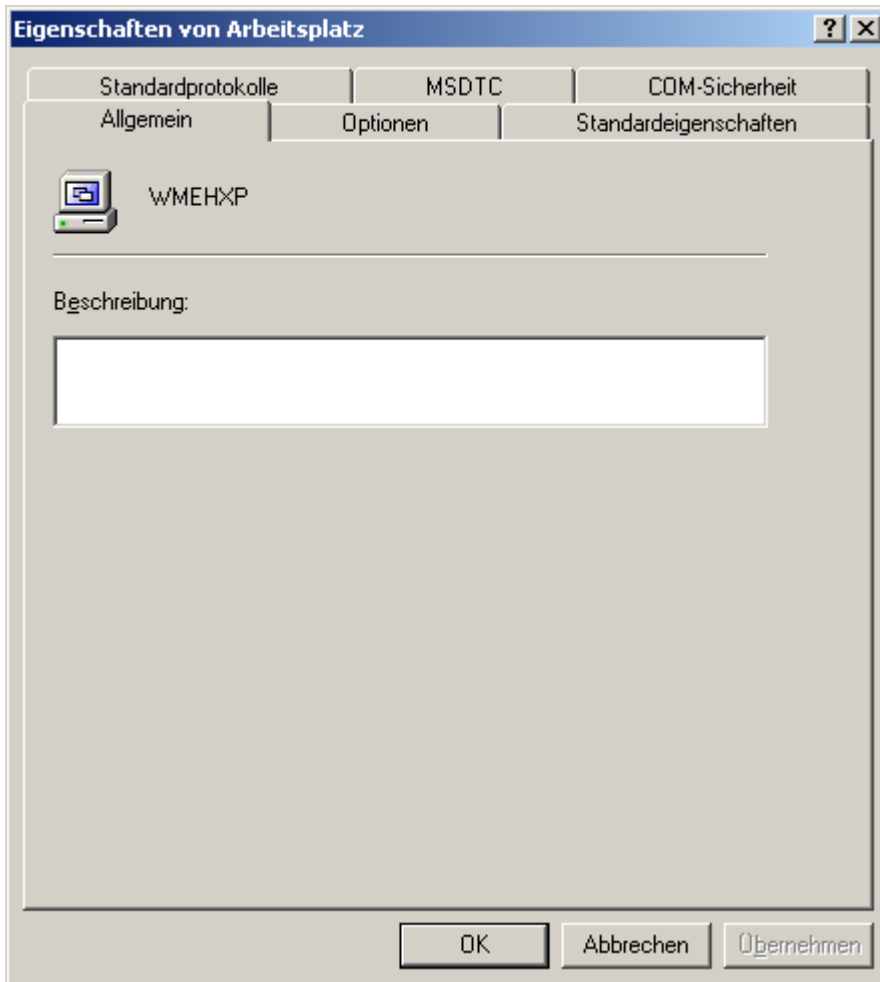


Abbildung 3: Startseite von „Eigenschaften von Arbeitsplatz“

2.3. Standardeigenschaften einstellen

- Reiter „Standardeigenschaften“ auswählen
- DCOM auf diesem Computer aktivieren
- Standardauthentifizierungsebene: Keine
- Standardidentitätswechselebene: Identität annehmen

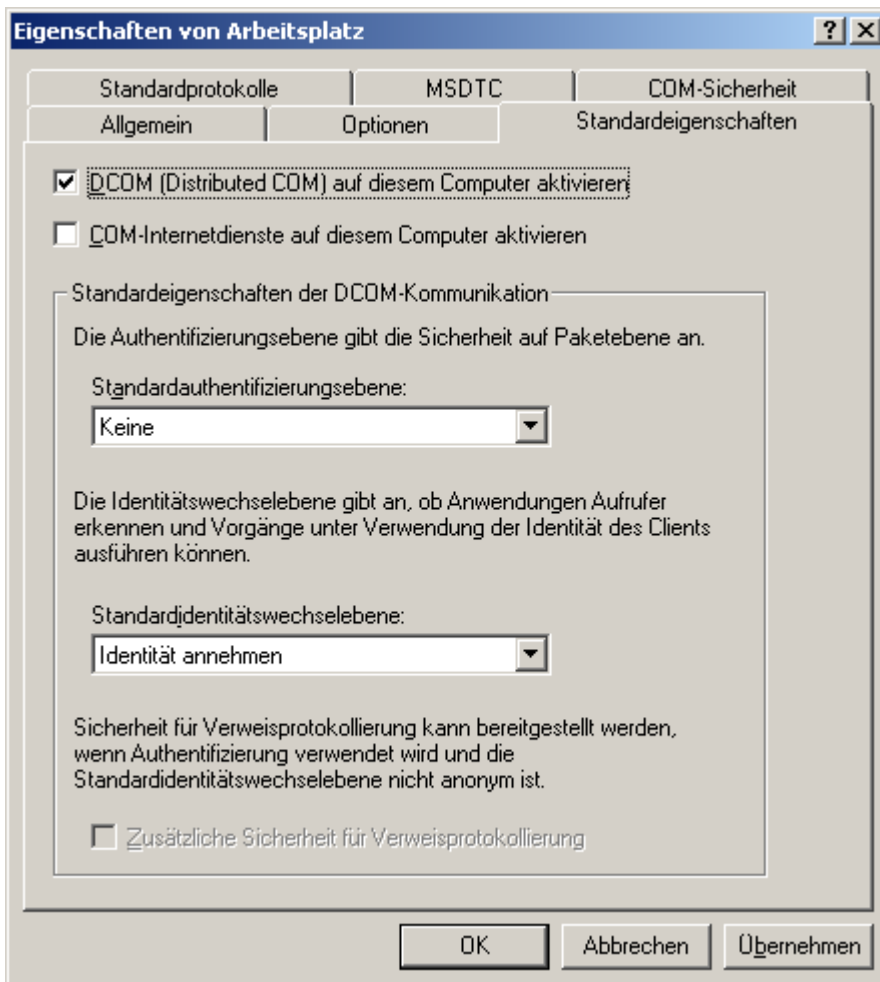


Abbildung 4: Reiter „Standardeigenschaften“



Hinweis:

Standardauthentifizierungsebene: Gibt an, wann die Authentifizierung durchgeführt werden soll (nie, beim Verbinden, für jedes Paket, usw.)

Standardidentitätswechselebene: Gibt an, ob Anwendungen Aufrufer erkennen und Vorgänge unter Verwendung der Identität des Clients ausführen können.

2.4. Standardprotokolle einstellen

- Reiter „Standardprotokolle“ auswählen
- Überprüfen, dass an erster Stelle „Verbindungsorientiertes TCP/IP“ eingestellt ist



Abbildung 5: Reiter „Standardprotokolle“



Hinweis:

Die Protokolle werden in der Reihenfolge von Windows durchprobiert, in der Sie hier dargestellt sind. Wenn „Verbindungsorientiertes TCP/IP“ nicht an erster Stelle steht, kommt es zu Verzögerungen. Dauert der Verbindungsaufbau länger, als für den Server-Aufbau zur Verfügung gestellt wird, kann der Server nicht gestartet werden.

Eine hohe Anzahl eingetragener DCOM-Protokolle führen bei einem Verbindungsabbruch zu unnötigen Verzögerungen. Unbenötigte Einträge sollten deshalb entfernt werden.

2.5. COM-Sicherheit einstellen

- Reiter „COM-Sicherheit“ auswählen
- Zugriffsberechtigungen: „Limits bearbeiten...“-Taste drücken
- Benutzername „ANONYMOUS-ANMELDUNG“, „INTERAKTIV“, „Jeder“, „NETZWERK“ und „SYSTEM“ hinzufügen (siehe Hinweis)
- Für diese Benutzernamen „Lokaler Zugriff“ und „Remotezugriff“ zulassen
- „OK“-Taste drücken

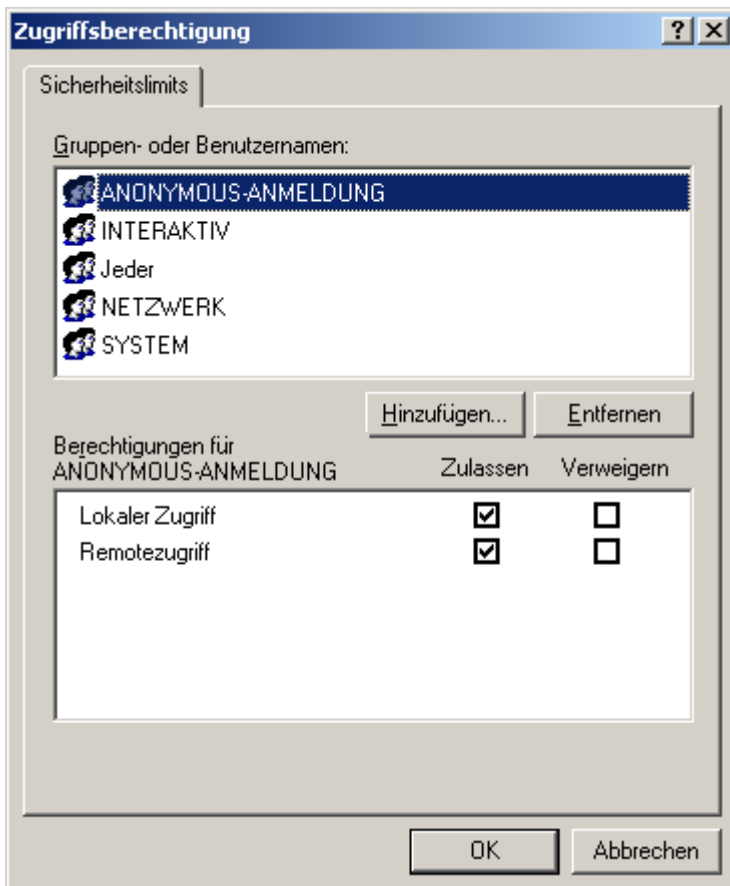


Abbildung 6: Einstellen der Zugriffsberechtigungen



Hinweis:

Wenn ein gewünschter Gruppen-, oder Benutzername nicht in der Auswahl auftaucht kann dieser folgendermaßen hinzugefügt werden:

- „Hinzufügen“-Taste drücken
- „Erweitert“-Taste drücken
- „Jetzt suchen“-Taste drücken
- Gruppen-, oder Benutzername markieren (Mehrfachauswahl mit gedrückter „Strg“-Taste)
- „OK“-Taste drücken



Hinweis:

Die Benutzergruppe „Jeder“ enthält alle Benutzer (lokal und Domäne). Sie können die Berechtigungen auch für eine Gruppe anlegen (z.B. „OPC-User“) und in diese Gruppe alle OPC-Benutzer aufnehmen. Diese Gruppe muss dann auf Server-Rechner und Client-Rechner existieren. Windows erlaubt bei DCOM-Kommunikation keine leeren Passwörter.

- Start und Aktivierungsberechtigungen: „Limits bearbeiten...“-Taste drücken
- Benutzername „INTERAKTIV“, „Jeder“, „NETZWERK“ und „SYSTEM“ hinzufügen
- Für diese Benutzer und den Administrator „Lokaler Start“, „Remotestart“, „Lokale Aktivierung“ und „Remoteaktivierung“ zulassen
- „OK“-Taste drücken

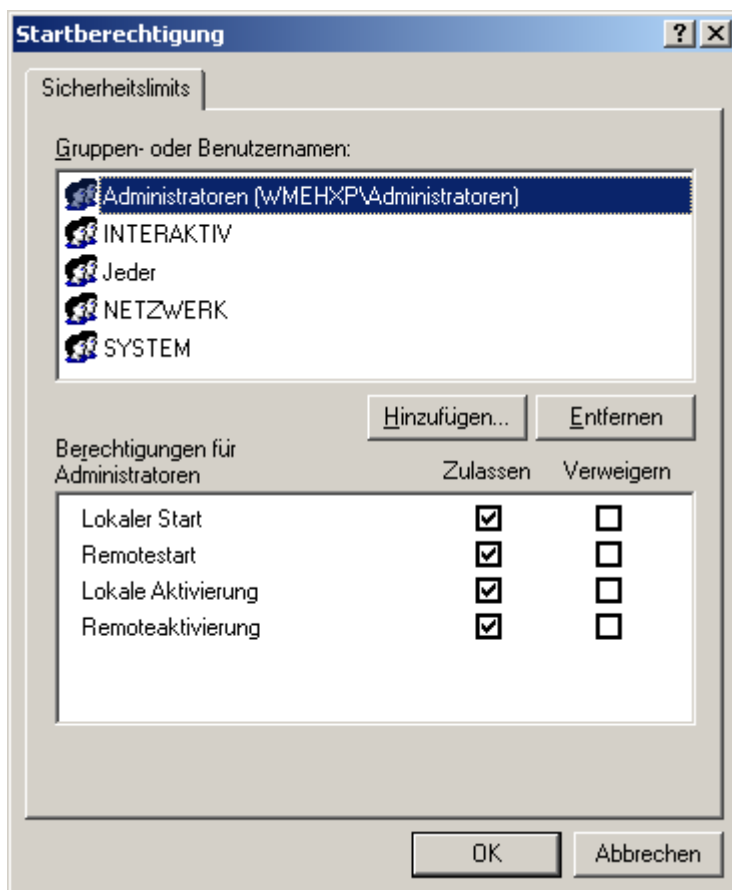


Abbildung 7: Einstellen der Startberechtigung

- Zugriffsberechtigungen: „Standard bearbeiten...“-Taste drücken
- Benutzername „INTERAKTIV“, „Jeder“, „NETZWERK“ und „SYSTEM“ hinzufügen
- Für diese Benutzer und den Administrator „Lokaler Zugriff“ und „Remotezugriff“ zulassen
- „OK“-Taste drücken

- Start und Aktivierungsberechtigungen: „Standard bearbeiten...“-Taste drücken
- Benutzername „INTERAKTIV“, „Jeder“, „NETZWERK“ und „SYSTEM“ hinzufügen
- Für diese Benutzer und den Administrator „Lokaler Start“, „Remotestart“, „Lokale Aktivierung“ und „Remoteaktivierung“ zulassen
- „OK“-Taste drücken

- Dialog „Eigenschaften von Arbeitsplatz“: „OK“-Taste drücken

3. DCOM-Einstellungen für anwendungsspezifische Sicherheitsparameter

Führen Sie die nachfolgenden Schritte für Ihre OPC-Server und OPCenum.exe auf dem Server-Rechner aus.

3.1. Öffnen des Eigenschaftsdialogs für einen OPC-Server

- DCOM Config starten (siehe Kapitel 2 DCOM-Einstellungen für systemweite Sicherheitsparameter)
- „Konsolenstamm / Komponentendienste / Computer / Arbeitsplatz / DCOM-Konfiguration“ in Baumansicht auswählen
- DCOM-Server auswählen (rechte Seite)
- Kontextmenü öffnen (rechte Maustaste) → Eigenschaften

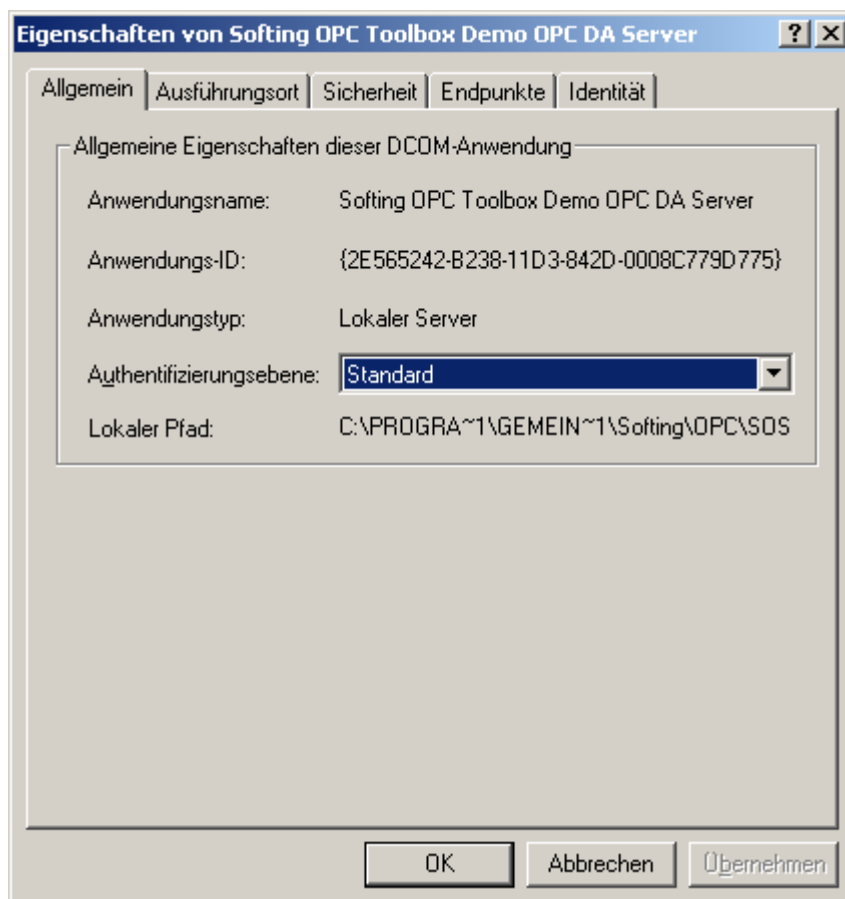


Abbildung 8: Anwendungsspezifische Startseite der DCOM-Konfiguration

3.2. Identität

- Reiter „Identität“ auswählen
- „Interaktiver Benutzer“ auswählen

Eigenschaften von OpcEnum

Allgemein | Ausführungsort | Sicherheit | Endpunkte | **Identität**

Welches Benutzerkonto soll verwendet werden, um diese Anwendung auszuführen?

☒ **Interaktiver Benutzer**

☐ Benutzer, der die Anwendung startet

☐ Dieser Benutzer:

Benutzer:

Kennwort:

Kennwort bestätigen:

☐ Systemkonto (nur für Dienste)

OK Abbrechen Übernehmen

Abbildung 9: Einstellen der Identität



Hinweis:

Wenn ein OPC-Server als „Dienst“ läuft, sind die Zeilen „Interaktiver Benutzer“ und „Benutzer, der die Anwendung startet“ ausgegraut. Wählen Sie in diesem Fall „Dieser Benutzer“, und tragen Sie einen Benutzer ein (bevorzugt aus der Gruppe „OPC-User“) (siehe Hinweis in Kapitel 2 „DCOM-Einstellungen für systemweite Sicherheitsparameter“)

3.3. Sicherheitseinstellungen vornehmen

- Reiter „Sicherheit“ auswählen
- Start- und Aktivierungsberechtigungen: „Standard“ auswählen
- Zugriffsberechtigungen: „Standard“ auswählen
- Konfigurationsberechtigungen: „Anpassen“ auswählen und „Bearbeiten...“-Taste drücken
- Benutzername „INTERAKTIV“, „Jeder“, „NETZWERK“ und „SYSTEM“ hinzufügen
- Für diese Benutzer und den Administrator „Vollzugriff“ und „Lesen“ zulassen
- „OK“-Taste drücken



Hinweis:

Damit OPC Server und OPC Client die Einstellungen von „dcomcnfg“ übernehmen, müssen diese neu gestartet werden.

4. Aktivierung des Gast-Zugangs

Dieses Kapitel ist nur für Windows XP relevant. Die Standardinstallation von XP authentifiziert Benutzer von entfernten Rechnern als Gast. Das bedeutet, dass sich ein DCOM Client nicht zu einem Server verbinden kann, bis der Gast Zugang aktiviert ist und genügend Rechte hat um auf den Server zuzugreifen.

Die nachfolgenden Einstellungen sind auf dem Client-Rechner, und dem Server-Rechner durchzuführen.

- Windows-Startmenü öffnen
- „Einstellungen / Systemsteuerung“ auswählen
- „Verwaltung“ auswählen
- „Lokale Sicherheitsrichtlinie“ auswählen
- „Lokale Richtlinien / Sicherheitsoptionen“ in Baumansicht auswählen
- Doppelklick ausführen auf „Netzwerkzugriff: Modell für gemeinsame Nutzung und Sicherheitsmodell für lokale Konten“
- „Klassisch - lokale Benutzer authentifizieren sich als sie selbst“ auswählen
- Doppelklick ausführen auf „Netzwerkzugriff: Die Verwendung von ‚Jeder‘-Berechtigungen für anonyme Benutzer ermöglichen“
- „Aktiviert“ auswählen

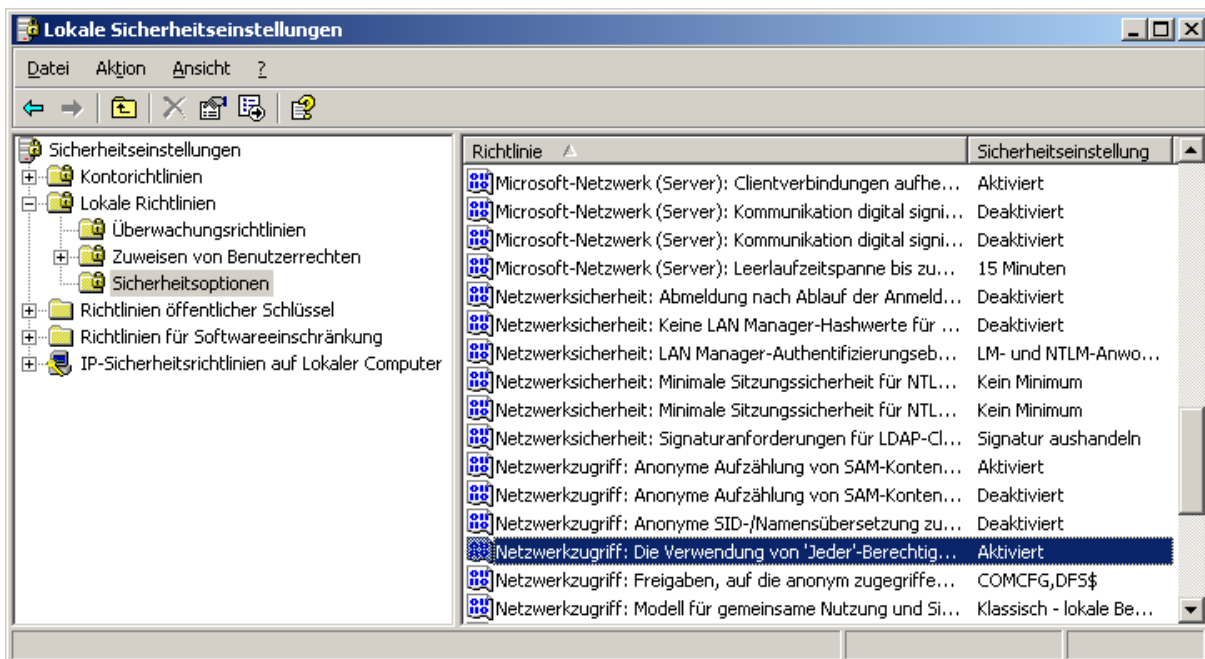


Abbildung 10: Einstellen der lokalen Sicherheitseinstellungen

5. Konfiguration der Windows-Firewall

Dieses Kapitel bezieht sich auf die Firewall von Windows XP SP2. Die Einstellungen beziehen sich sinn- gemäß aber auch auf jede andere Firewall. Die Konfiguration ist auf dem Client-Rechner, und dem Server- Rechner durchzuführen.

5.1. „Windows Firewall“-Konfigurator starten

- Windows-Startmenü öffnen
- „Einstellungen / Systemsteuerung“ auswählen
- „Windows-Firewall“ auswählen



Abbildung 11: Die Windows Firewall

5.2. Ausnahmen festlegen

- Reiter „Ausnahmen“ auswählen
- „Programm...“-Taste drücken
- Die folgenden Programme hinzufügen
 - o Alle OPC-Clients / OPC-Server
 - o Microsoft Management Console
 - o „OPCEnum.exe“ (Windows/System32)



Hinweis:

Im Dialog „Programm hinzufügen“ werden nicht alle Applikationen angezeigt. Weitere können über die „Durchsuchen“-Taste gefunden werden.



Hinweis:

In die Ausnahmeliste werden nur *.exe – Files aufgenommen. Bei einem In-Process Server wählen Sie bitte die Anwendung, die den Server aufruft.

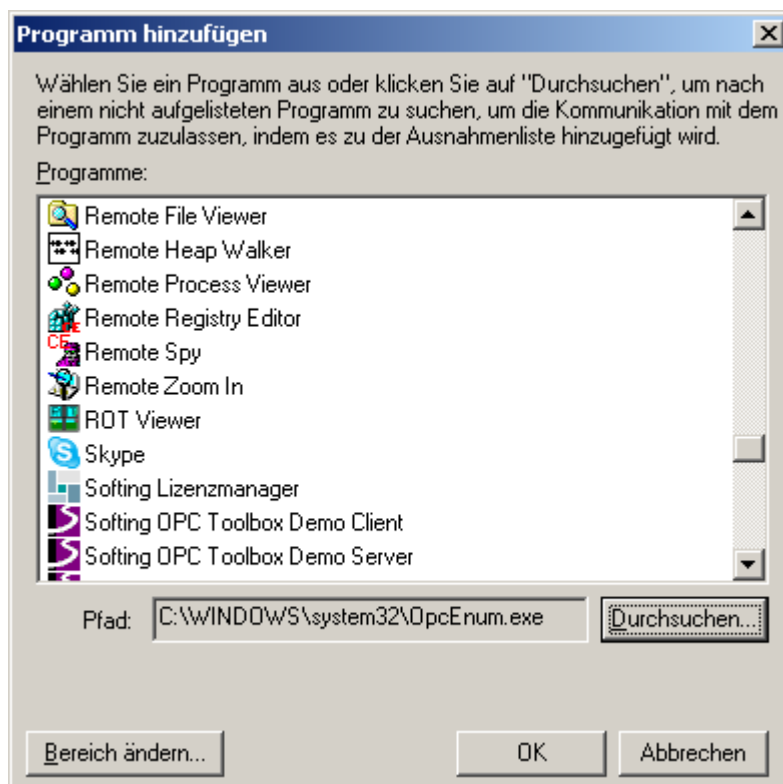


Abbildung 12: Ausnahmen festlegen

5.3. Port freigeben

- Reiter „Ausnahmen“ auswählen
- „Port ...“-Taste drücken
- Die folgenden Einstellungen vornehmen:
 - o Name: „DCOM“
 - o Portnummer: „135“
 - o Radiobutton „TCP“ auswählen
- „OK“-Taste drücken

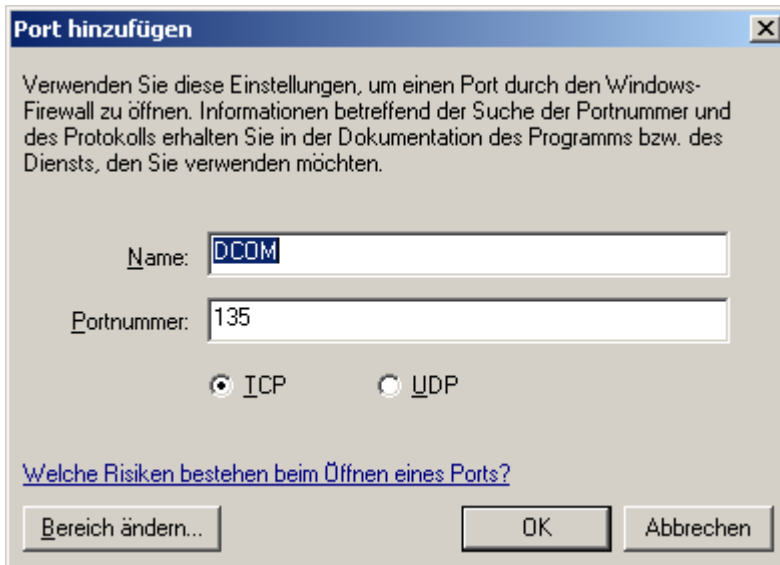


Abbildung 13: Portfreigabe für DCOM



Hinweis:

Das Öffnen des Ports 135 stellt eine kritische Sicherheitslücke dar. Dadurch wird Applikationen über das Netzwerk ermöglicht, „Remote Procedure Calls“ durchzuführen, und somit Windows-Komponenten zu beeinflussen. Dies stellt für viele Computer-Viren ein Einfallstor dar. Bitte stellen Sie auf jeden Fall sicher, das zwischen Ihrem Firmennetzwerk und dem Internet der Port 135 geschlossen bleibt.

6. DCOM unter Windows CE

Bei Windows CE werden die Sicherheitseinstellungen für rechnerübergreifende OPC-Kommunikation noch restriktiver gehandhabt. Außerdem steht kein Programm zur DCOM Konfiguration zur Verfügung. Daher ist hier keine generische Beschreibung möglich. Bitte wenden Sie sich bei Fragen an unseren Support (support.automation@softing.com).

7. OPC Connector Tool „OPC-Tunnel“

Der OPC Tunnel ermöglicht als „DCOM Bypass“ die Kommunikation zwischen OPC Komponenten auf vernetzten Rechnern. Dazu wird OPC Tunnel sowohl auf dem OPC Client Rechner, als auch auf dem OPC Server Rechner installiert.

Die Kommunikation zwischen den client- und server-seitigen OPC Tunnel Installationen erfolgt über eine TCP/IP Verbindung, die optional verschlüsselt werden kann. Somit werden die Daten, die zwischen Client und Server Applikationen ausgetauscht werden über TCP/IP „getunnelt“. DCOM wird komplett umgangen.

Die Konfiguration erfolgt über einen selbsterklärenden Assistenten. Im Wesentlichen werden dabei die IP-Adresse des Server Computers und ein Port für die TCP/IP Kommunikation definiert.

Der OPC Tunnel steht für Windows NT4, 2000, XP, 2003 und Windows CE zur Verfügung und unterstützt Data Access 1.0a, 2.05 und 3.0, sowie Alarms&Events 1.10.

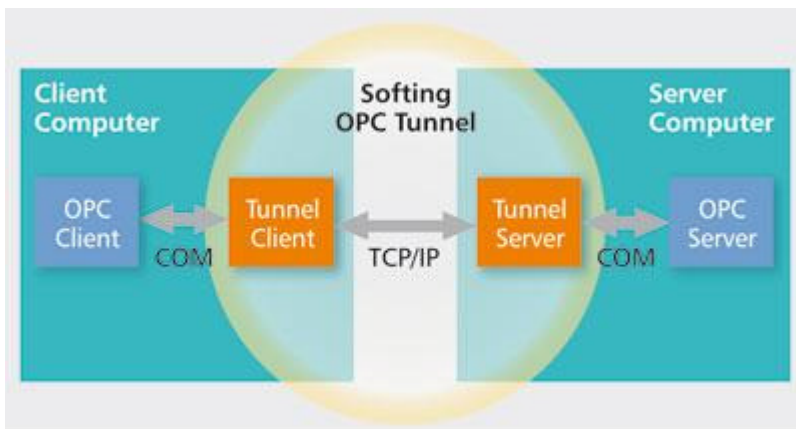


Abbildung 14: Rechnerübergreifende Kommunikation mit OPC Tunnel