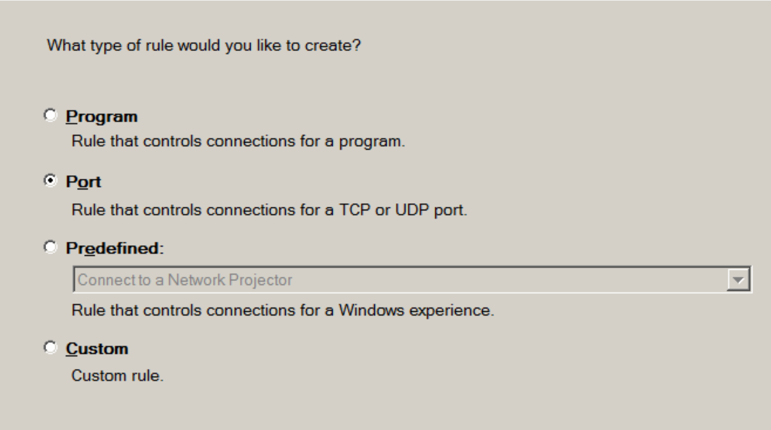
This document provides detailed DCOM configuration for setting up one or more machines for using Total Vu as an OPC Server on a Windows 7 machine.

1. Firewall Settings

Go to Start ->Control Panel->Windows Firewall->Advanced Settings. Inbound and Outbound rules need to be defined for DCOM Port 135, OPCEnum.exe, and TotalVu.exe .

DCOM Port 135 Inbound Rule for TCP

Right-click on Inbound Rules, select New Rule…, select Port for Rule Type, then click Next>



What type of rule would you like to create?

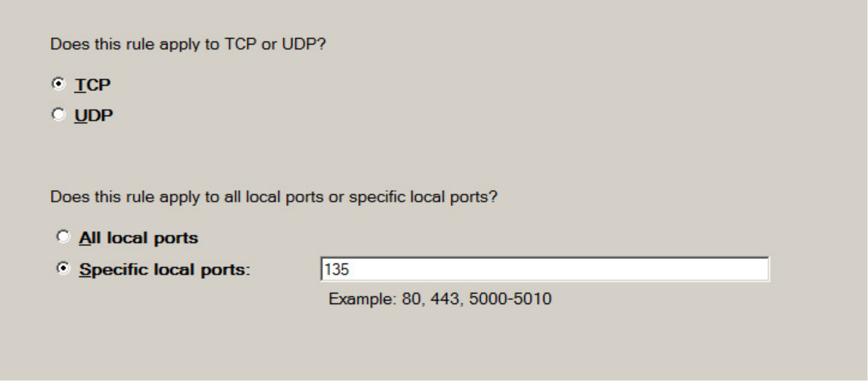
○ **Program**
Rule that controls connections for a program.

● **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Select TCP and specify 135 for the Specific Local Ports, then click Next>



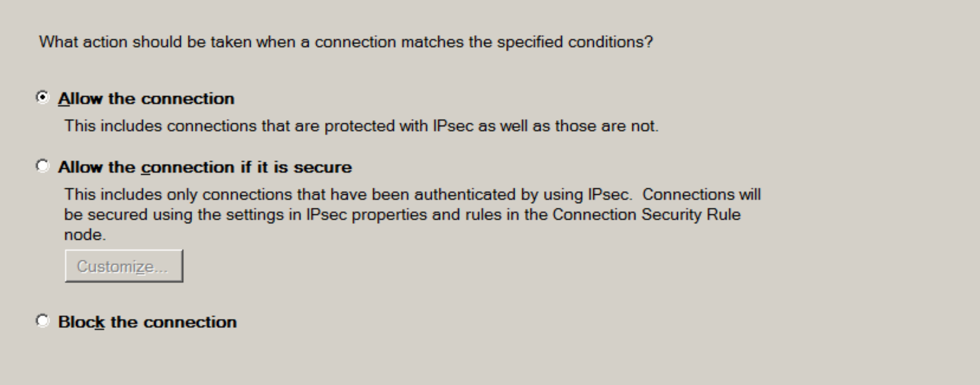
Does this rule apply to TCP or UDP?

● **TCP**
○ **UDP**

Does this rule apply to all local ports or specific local ports?

○ **All local ports**
● **Specific local ports:** 135
Example: 80, 443, 5000-5010

Select Allow the connection, then click Next>



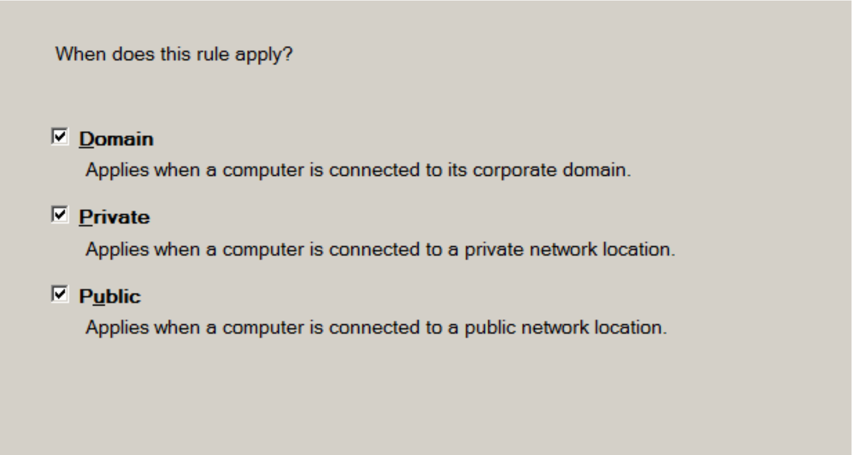
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Check Domain, Private, and Public, then click Next>



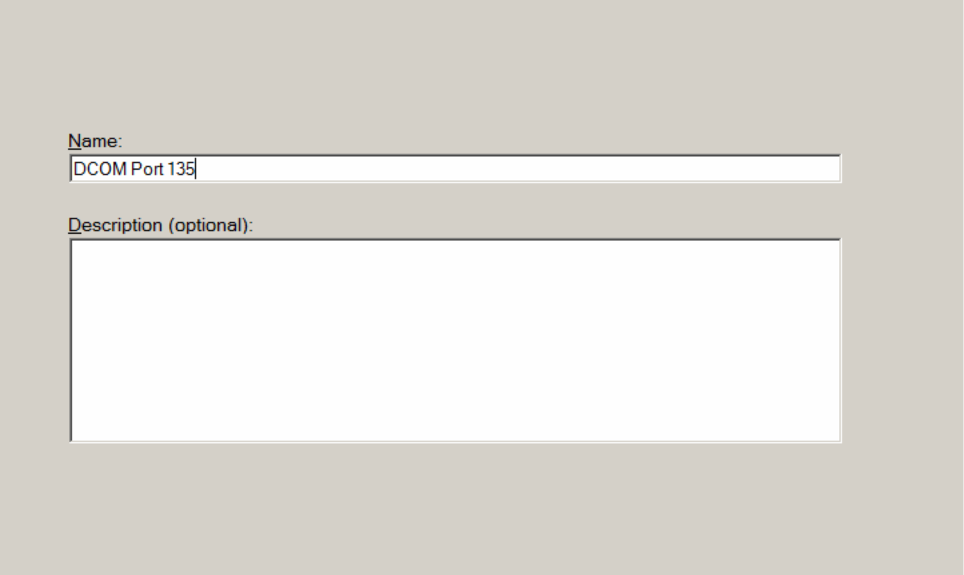
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Enter a name for this Inbound Rule (such as DCOM Port 135) and click Finish



Name:
DCOM Port 135

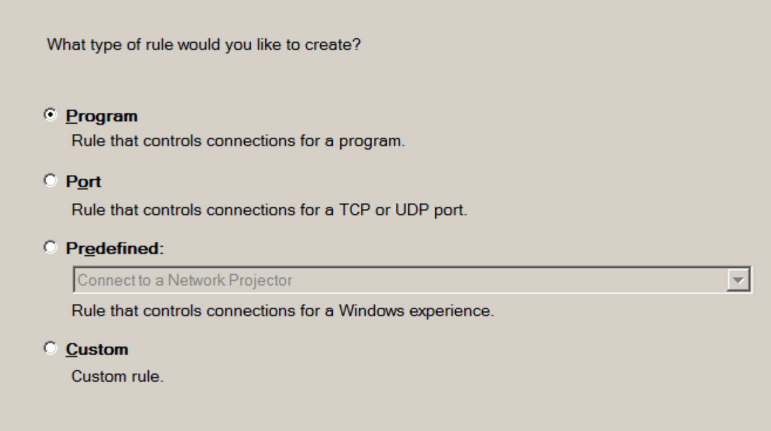
Description (optional):

DCOM Port 135 Inbound Rule for UDP

To create an Inbound rule for Port 135 and UDP Protocol, repeat the steps above but select UDP for Port 135.

OPCEnum Inbound Rule

To create an Inbound rule for OPCEnum.exe, right-click on Inbound Rules, select New Rule…, select Program for Rule Type, then click Next>



What type of rule would you like to create?

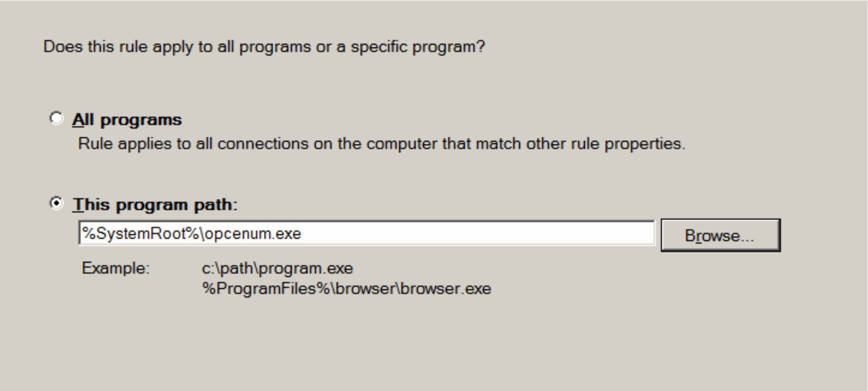
● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Select This program path and use the Browse… button to locate opcenum.exe in the C:\Windows folder, then click Next>



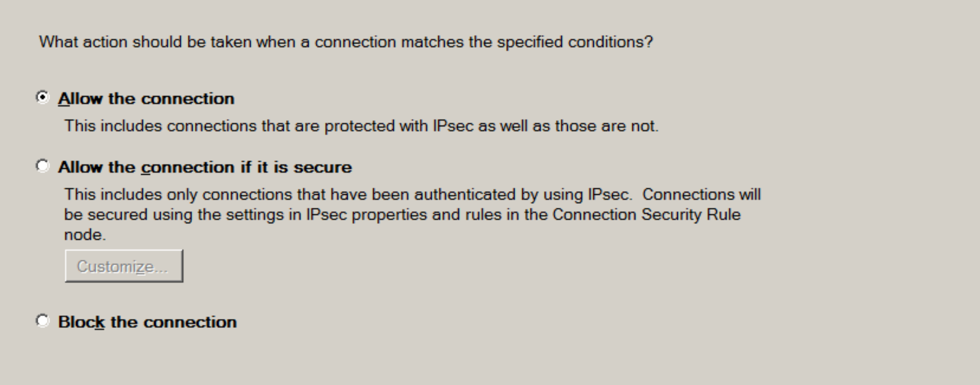
Does this rule apply to all programs or a specific program?

○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**
%SystemRoot%\opcenum.exe

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Select Allow the connection, then click Next>



What action should be taken when a connection matches the specified conditions?

● **Allow the connection**

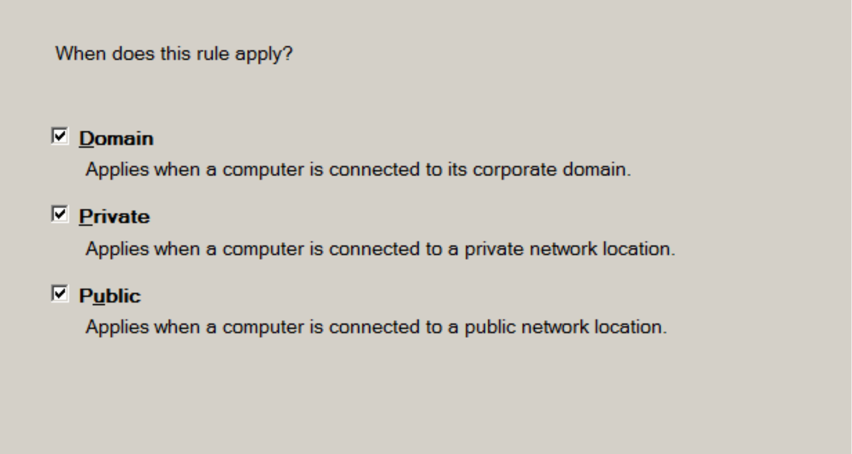
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**

This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Check Domain, Private, and Public, then click Next>



When does this rule apply?

☑ **Domain**

Applies when a computer is connected to its corporate domain.

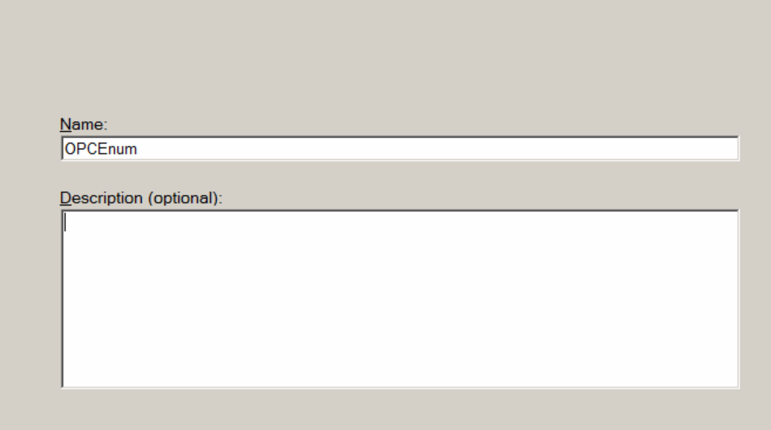
☑ **Private**

Applies when a computer is connected to a private network location.

☑ **Public**

Applies when a computer is connected to a public network location.

Enter a name for this Inbound rule (such as OPCEnum), then click Finish.

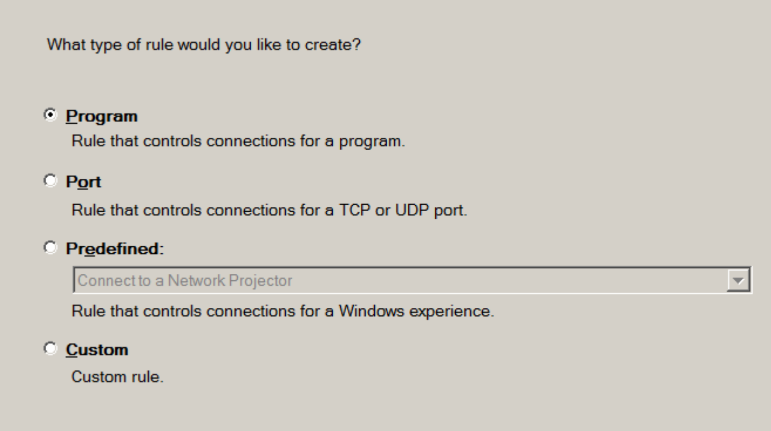


Name: OPCEnum

Description (optional):

Total Vu Inbound Rule

To create an Inbound rule for TotalVu.exe, right-click on Inbound Rules, select New Rule…, select Program for Rule Type, then click Next>



What type of rule would you like to create?

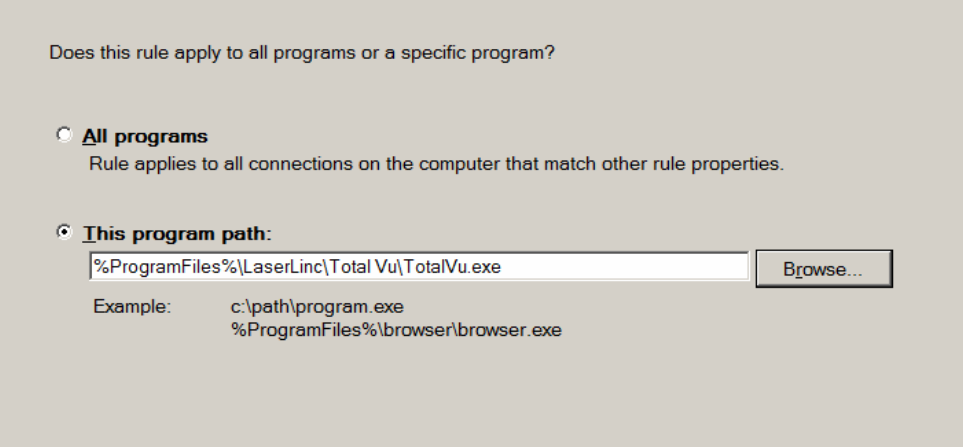
● **Program**
Rule that controls connections for a program.

○ **Port**
Rule that controls connections for a TCP or UDP port.

○ **Predefined:**
Connect to a Network Projector
Rule that controls connections for a Windows experience.

○ **Custom**
Custom rule.

Select This program path and use the Browse… button to locate TotalVu.exe in the Total Vu installation folder, then click Next>



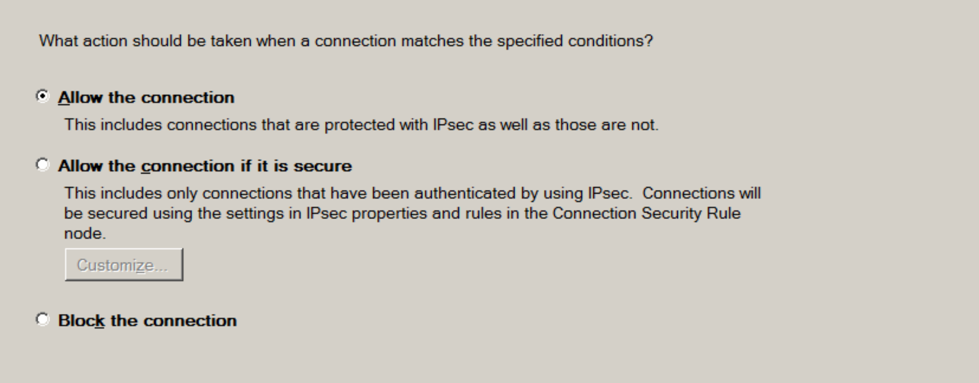
Does this rule apply to all programs or a specific program?

○ **All programs**
Rule applies to all connections on the computer that match other rule properties.

● **This program path:**
%ProgramFiles%\LaserLinc\Total Vu\TotalVu.exe

Example: c:\path\program.exe
%ProgramFiles%\browser\browser.exe

Select Allow the connection, then click Next>



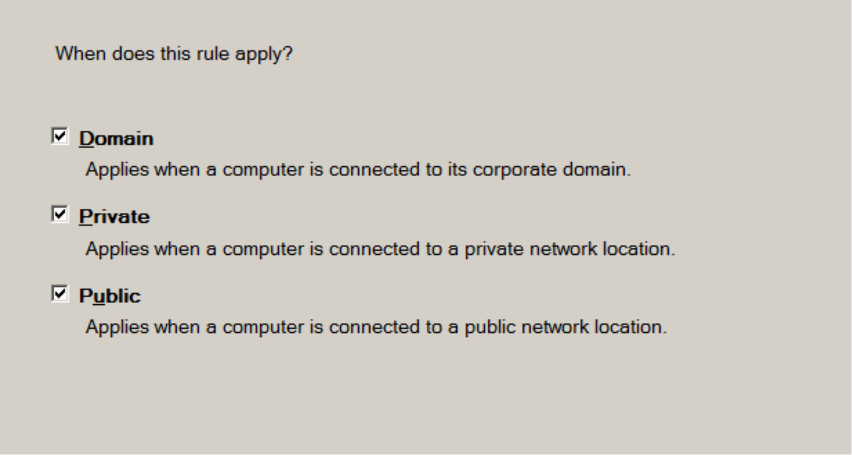
What action should be taken when a connection matches the specified conditions?

● **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

○ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

○ **Block the connection**

Check Domain, Private, and Public, then click Next>



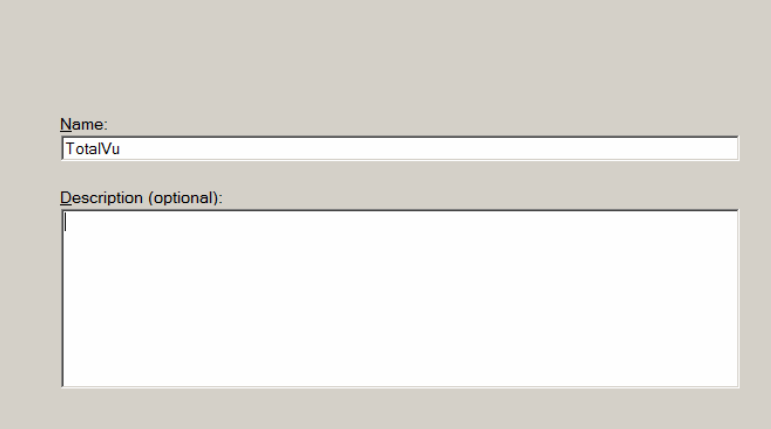
When does this rule apply?

☑ **Domain**
Applies when a computer is connected to its corporate domain.

☑ **Private**
Applies when a computer is connected to a private network location.

☑ **Public**
Applies when a computer is connected to a public network location.

Enter a name for this Inbound rule (such as TotalVu), then click Finish.



Name: TotalVu

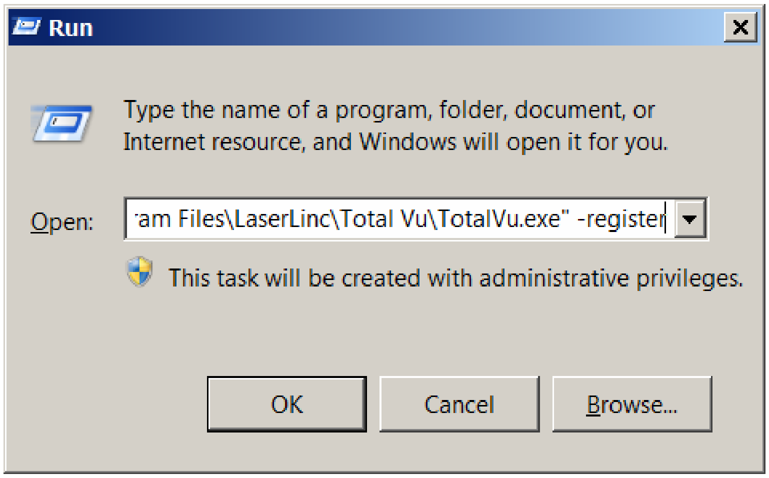
Description (optional):

Total Vu Outbound Rule

To create an Outbound rule for TotalVu.exe, right-click on Outbound Rules, select New Rule…, then follow the steps for creating the Total Vu Inbound Rule above.

2. Total Vu Server Registration

To register Total Vu as an OPC Server, go to Start->All Programs->Accessories->Run, click Browse to locate TotalVu.exe. Add the parameter -register and click OK. (Note: make sure there is a space between the enclosing " and the –register parameter).

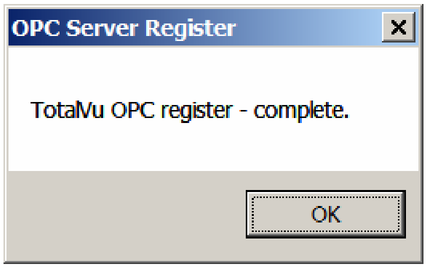


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: 'am Files\LaserLinc\Total Vu\TotalVu.exe" -register

This task will be created with administrative privileges.

Once registered, Total Vu will display the following message.



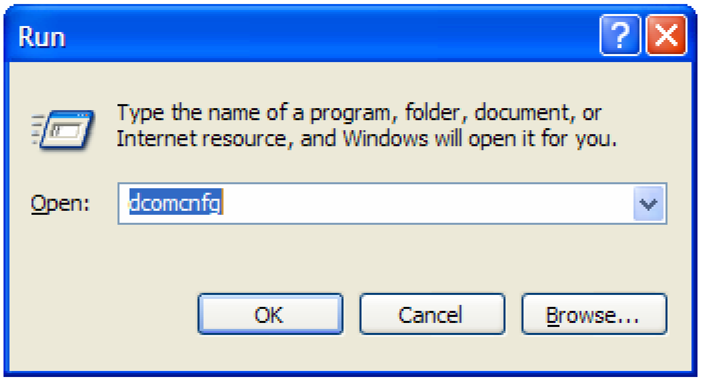
TotalVu OPC register - complete.

NOTE to RSView32 Users

Rockwell Automation RSView®32™ uses local registry entries to find information about OPC servers. Therefore, in a client-server PC network configuration, Total Vu must be installed and registered as an OPC Server on both the client and server PCs.

3. DCOM Settings

OPC uses ActiveX COM and DCOM for communication. To configure DCOM, go to Start->All Programs->Accessories->Run; enter dcomcnfg; then click OK.

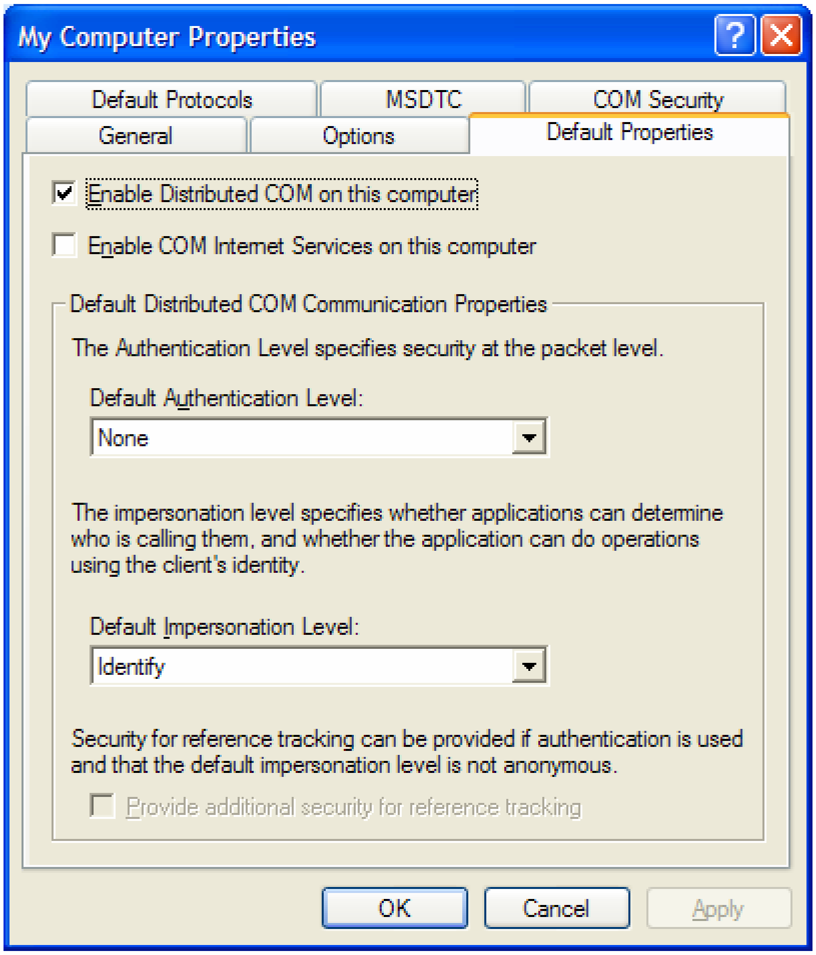


Run

Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: dcomcnfg

Go to Console Root->Component Services->Computers->My Computer. Right-click on My Computer and select Properties. Select the Default Properties Tab. Enable Distributed COM, set the Default Authentication Level to “None”, and set the Default Impersonation Level to “Identify”.



My Computer Properties

☑ Enable Distributed COM on this computer

☐ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level: None

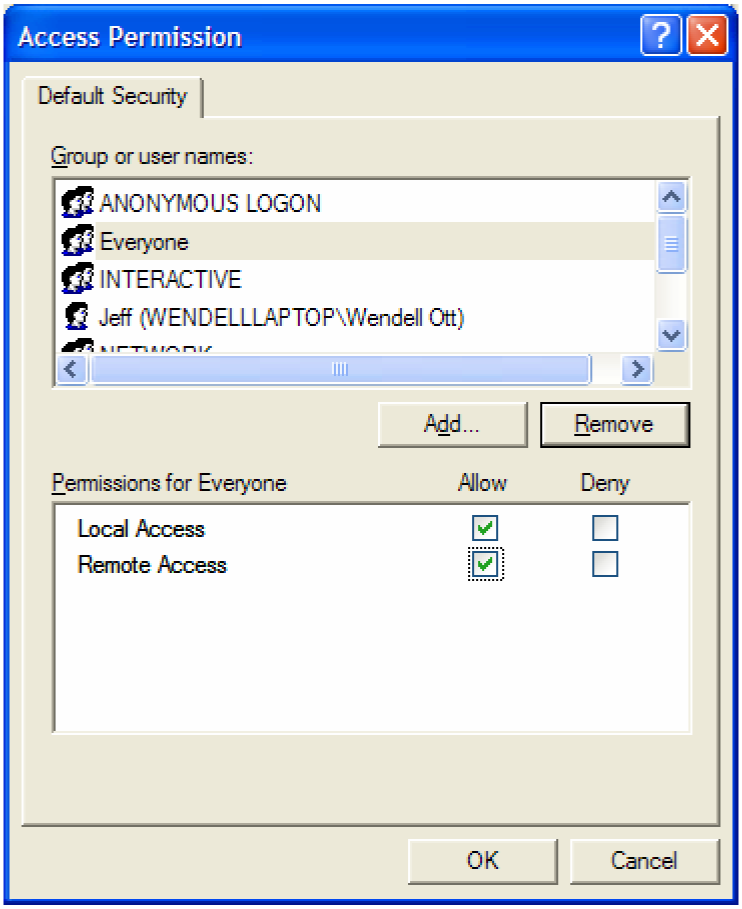
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity.

Default Impersonation Level: Identify

Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous.

☐ Provide additional security for reference tracking

Select the COM Security Tab. For each of Edit Limits… and Edit Default…, in Access Permissions and Launch and Activation Permissions, check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add… button.



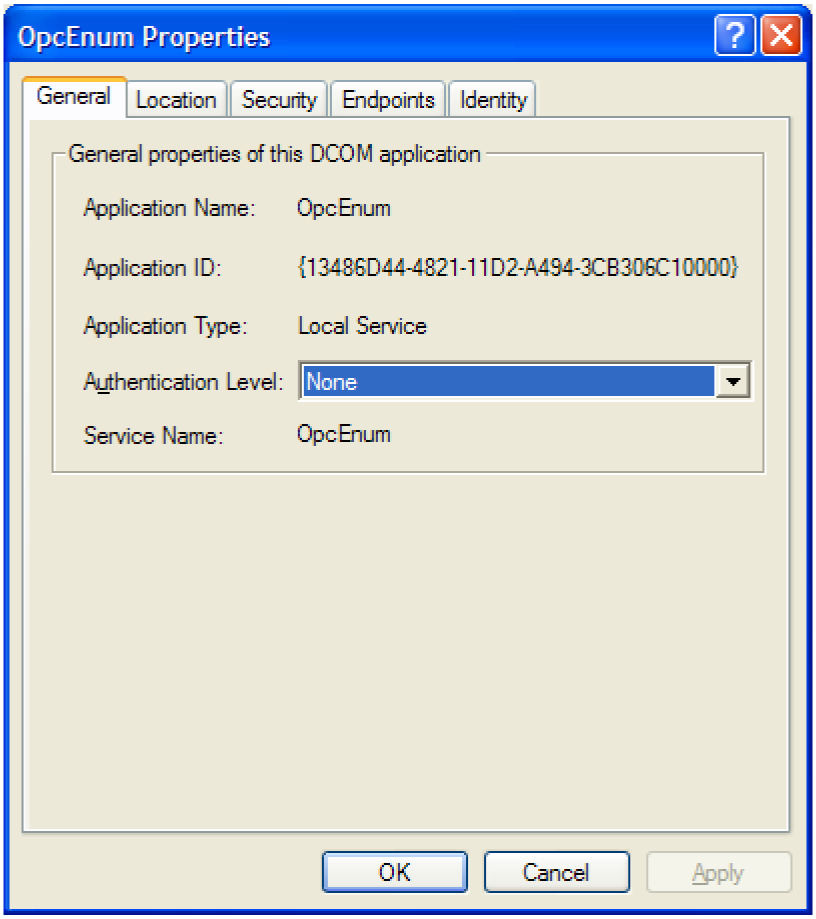
Group or user names:

- ANONYMOUS LOGON
- Everyone
- INTERACTIVE
- Jeff (WENDELLLAPTOP\Wendell Ott)
- NETWORK

Permissions for Everyone	Allow	Deny
Local Access	☑	☐
Remote Access	☑	☐

4. OpcEnum Properties

Run dcomcnfg, select Component Services->Computers->My Computer->DCOM Config. Right-click on OpcEnum and select Properties. On the General Tab, set Authentication Level to "None".



General properties of this DCOM application

Application Name: OpcEnum

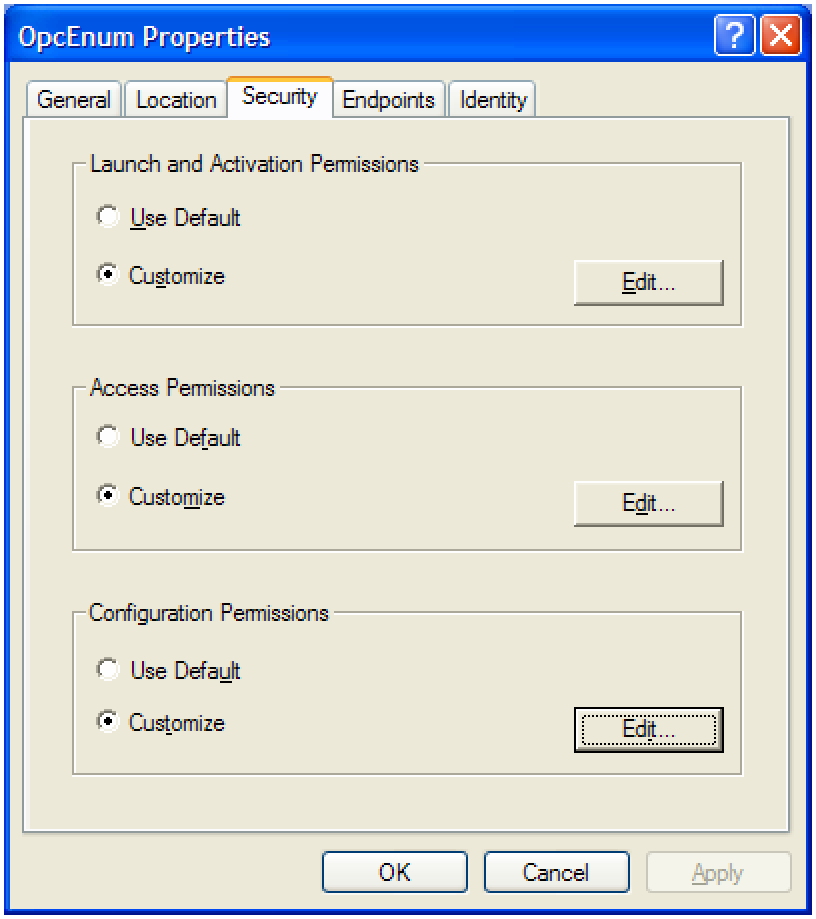
Application ID: {13486D44-4821-11D2-A494-3CB306C10000}

Application Type: Local Service

Authentication Level: None

Service Name: OpcEnum

Select the Security Tab. For Launch and Activation Permissions, Access Permissions, and Configuration Permissions, select Customize and then click the Edit… button.



Launch and Activation Permissions

○ Use Default

● Customize

Access Permissions

○ Use Default

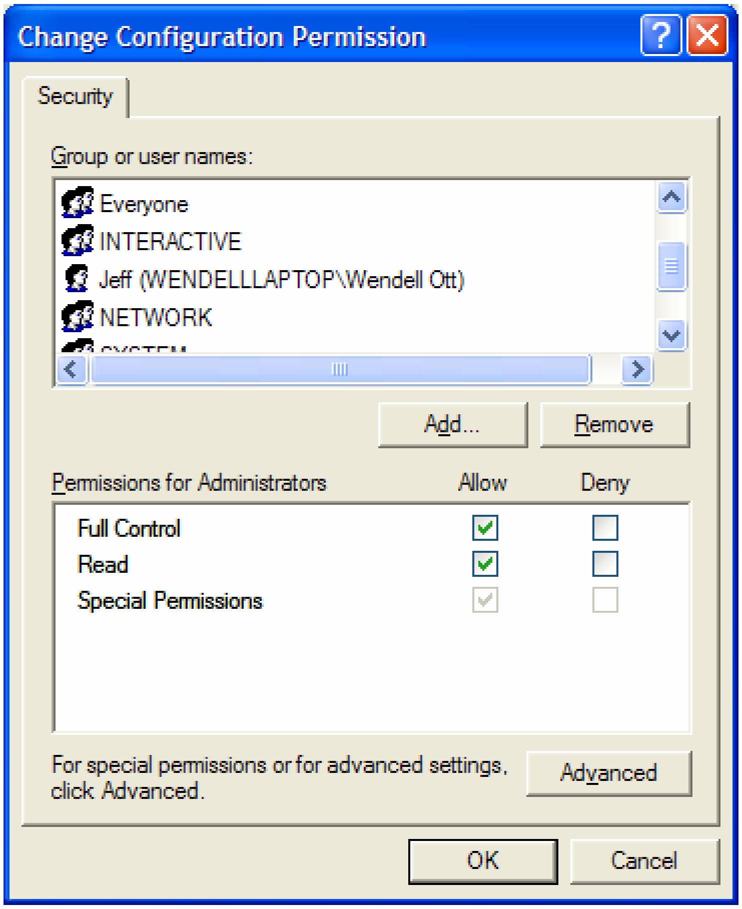
● Customize

Configuration Permissions

○ Use Default

● Customize

Check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add… button.



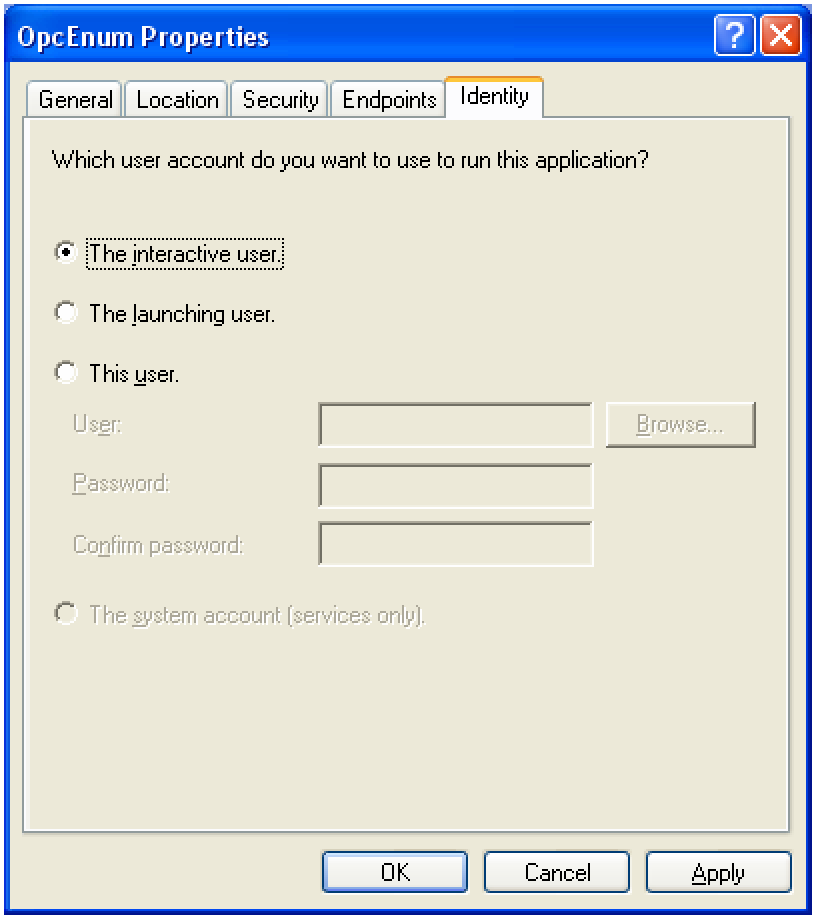
Group or user names:

- Everyone
- INTERACTIVE
- Jeff (WENDELLLAPTOP\Wendell Ott)
- NETWORK
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Read	☑	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Select the Identity Tab, and select The interactive user.



Which user account do you want to use to run this application?

● The interactive user.

○ The launching user.

○ This user.

User:

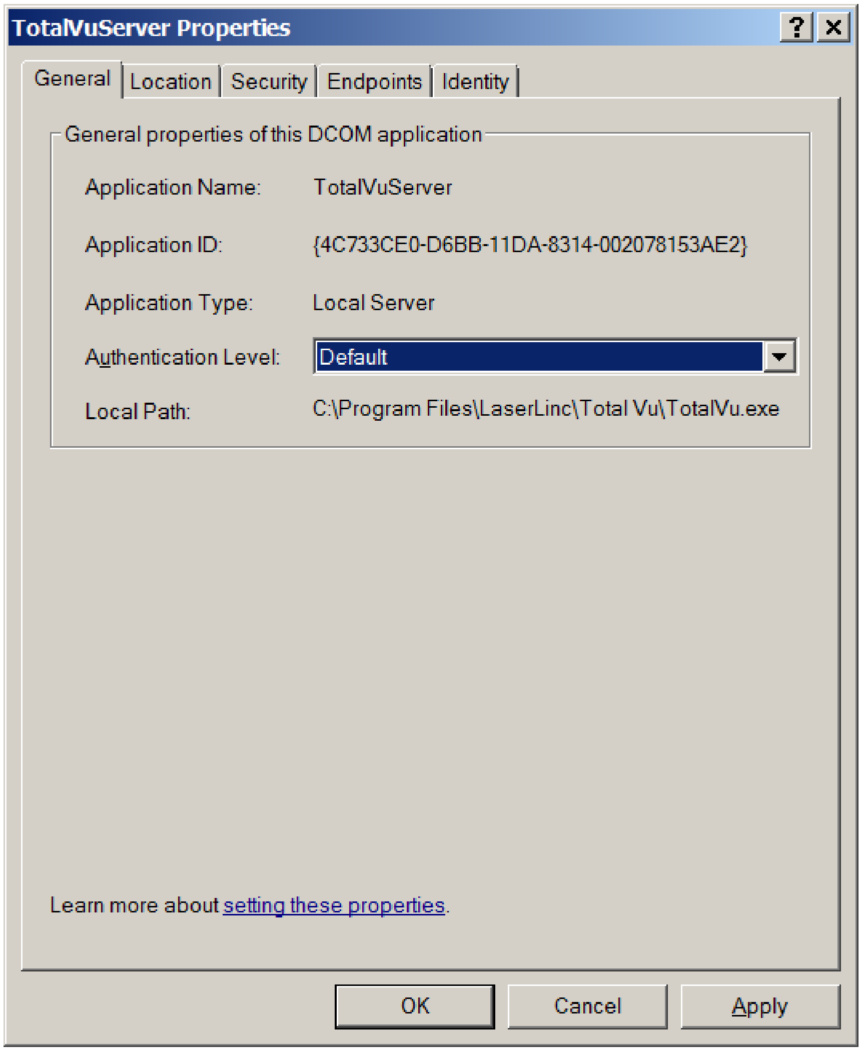
Password:

Confirm password:

○ The system account (services only).

5. TotalVuServer Properties

Right-click on TotalVuServer and select Properties. On the General Tab, set Authentication Level to "Default".



TotalVuServer Properties

General properties of this DCOM application

Application Name: TotalVuServer

Application ID: {4C733CE0-D6BB-11DA-8314-002078153AE2}

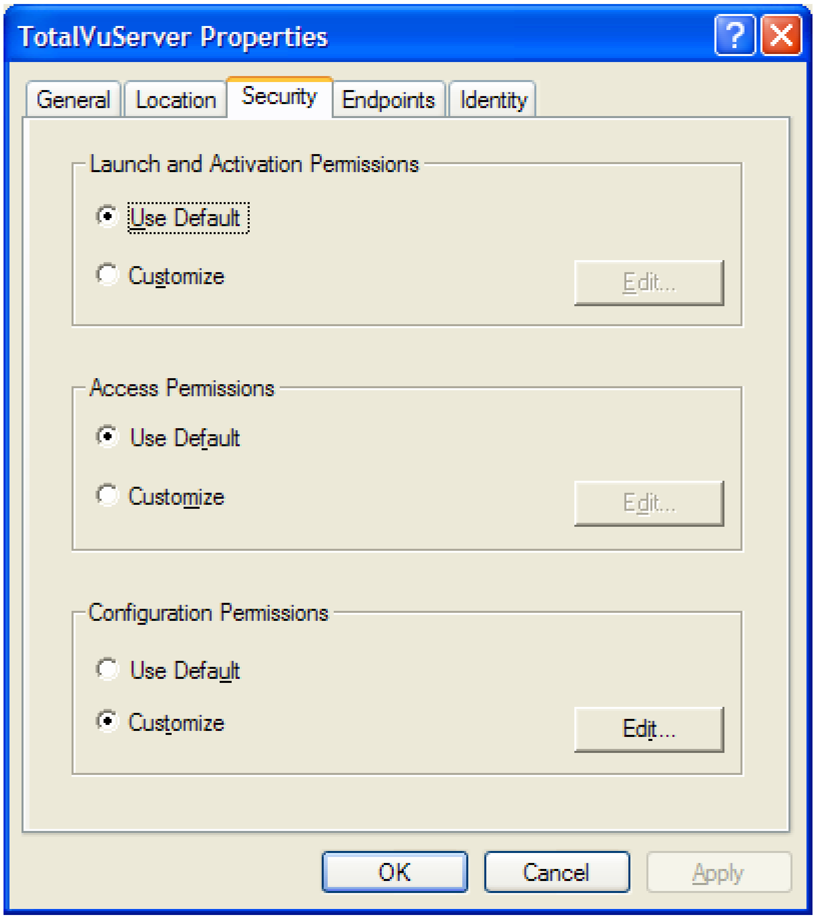
Application Type: Local Server

Authentication Level: Default

Local Path: C:\Program Files\LaserLinc\Total Vu\TotalVu.exe

Learn more about setting these properties.

Select the Security Tab. For Launch and Activation Permissions and Access Permissions, select Use Default. For Configuration Permissions, select Customize and then click the Edit… button.



TotalVuServer Properties

Launch and Activation Permissions

● Use Default

○ Customize

Access Permissions

● Use Default

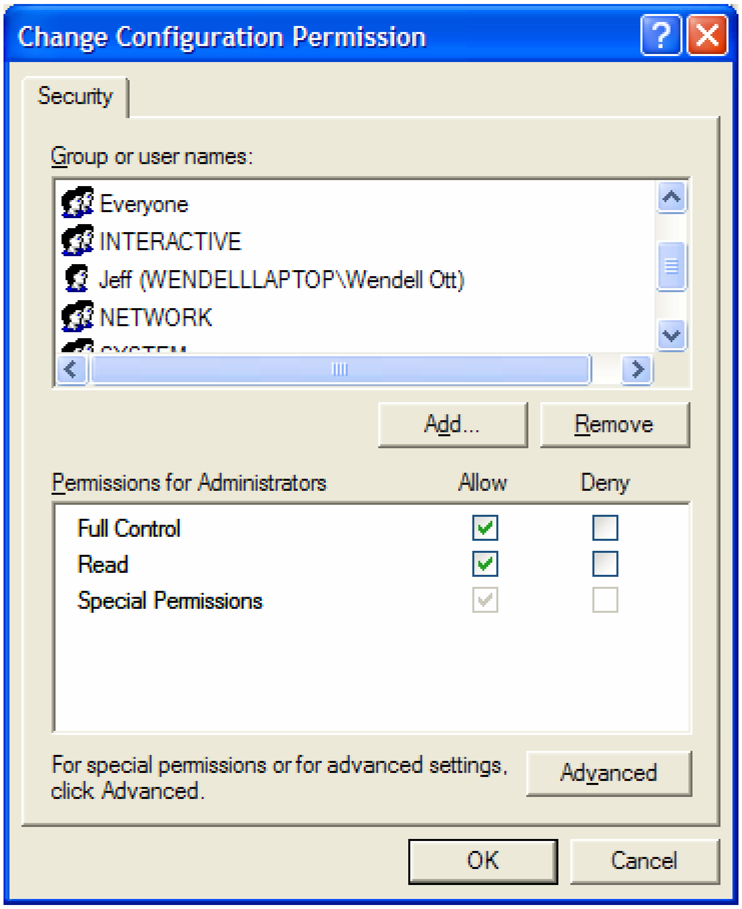
○ Customize

Configuration Permissions

○ Use Default

● Customize

Check all the Allow check boxes for the following Groups or User Names: ANONYMOUS LOGON, Everyone, Interactive, NETWORK, SYSTEM, and an Administrator account. If the Group or User Name is not in the list, add it using the Add… button.



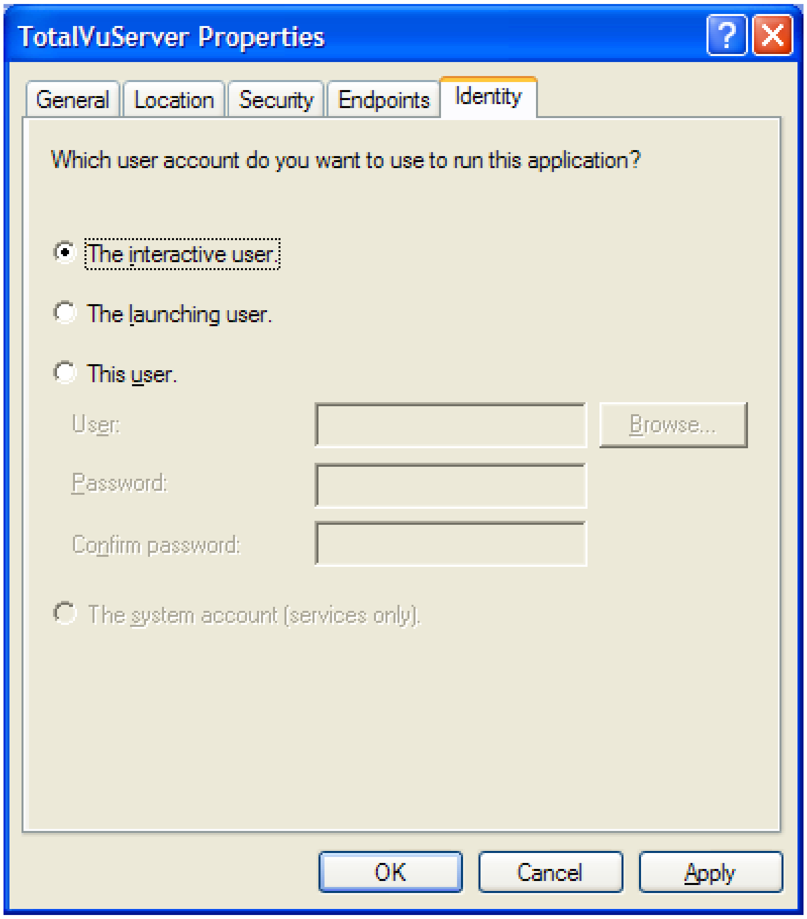
Group or user names:

- Everyone
- INTERACTIVE
- Jeff (WENDELLLAPTOP\Wendell Ott)
- NETWORK
- SYSTEM

Permissions for Administrators	Allow	Deny
Full Control	☑	□
Read	☑	□
Special Permissions	☑	□

For special permissions or for advanced settings, click Advanced.

Select the Identity Tab and select The interactive user.



TotalVuServer Properties

Which user account do you want to use to run this application?

● The interactive user.

○ The launching user.

○ This user.

User:

Password:

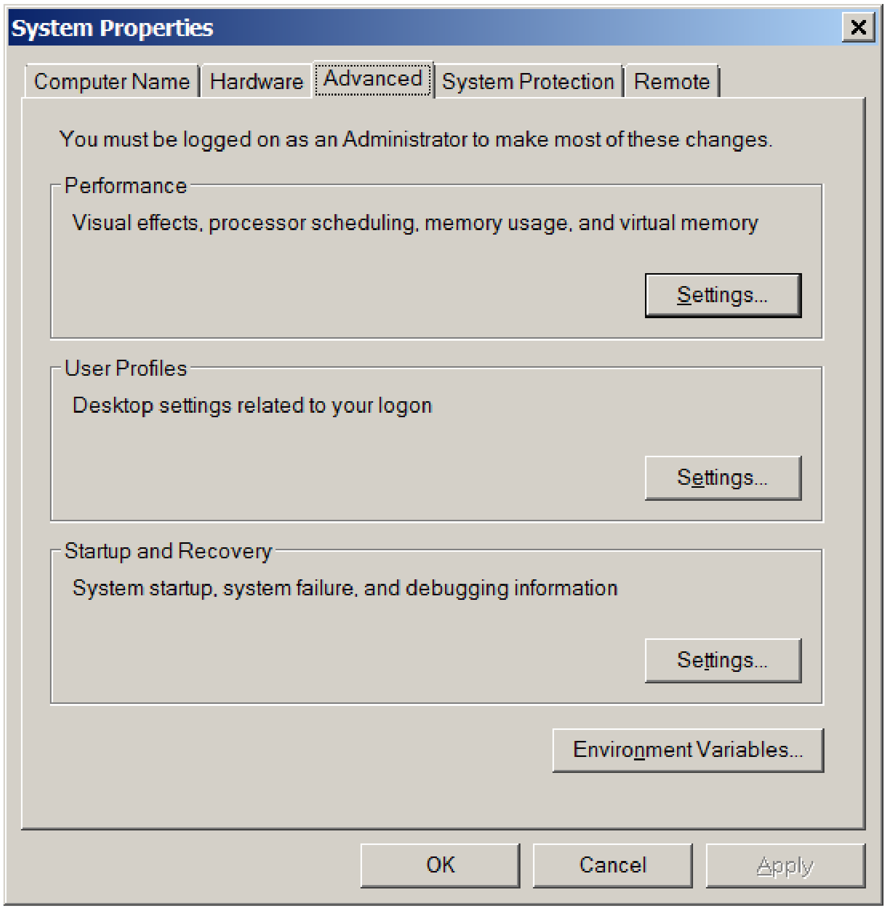
Confirm password:

○ The system account (services only).

6. Data Execution Prevention

Data Execution Prevention (DEP) is a set of hardware and software technologies that perform additional checks on memory to help prevent malicious code from running on a system. In Microsoft Windows XP, DEP must be disabled for OPC to function properly.

Go to Start, right-click on My Computer, and select Properties. Select the Advanced Tab and click on Settings under Performance.



You must be logged on as an Administrator to make most of these changes.

Performance

Visual effects, processor scheduling, memory usage, and virtual memory

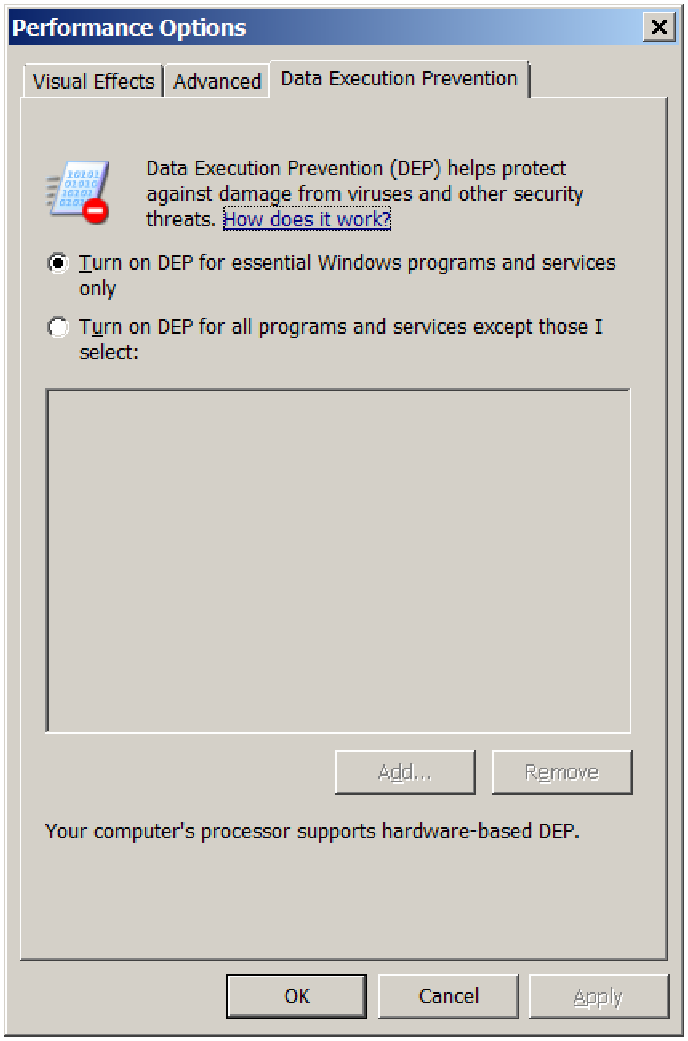
User Profiles

Desktop settings related to your logon

Startup and Recovery

System startup, system failure, and debugging information

Select the Data Execution Prevention tab, and select the “Turn on DEP for essential Windows programs and services only” radio button.



Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. How does it work?

● Turn on DEP for essential Windows programs and services only

○ Turn on DEP for all programs and services except those I select:

Your computer's processor supports hardware-based DEP.

7. Reboot

Reboot the machine to install the new DCOM settings. Once rebooted, OPC should function properly. In the event of problems, Matrikon offers several free tools from their web-site for diagnosing OPC/DCOM problems: www.matrikonopc.com.