

Microsoft Windows Security Configuration

Windows 7 and Server 2008 Configuration Guide

MatrikonOPC

Microsoft Windows Security Configuration

This manual is a product of Matrikon Inc.

Matrikon Inc.
Suite 1800, 10405 Jasper Avenue
Edmonton, AB T5J 3N4
Canada

Phone: +1.780.448.1010
Fax: +1.780.448.9191
www.matrikonopc.com

Document Revision History:

Date	Document Version	Description	Author
2013-01-14	1.0	Initial document.	TS
2013-04-05	1.1	Revisions.	TS

SOFTWARE VERSION

Version: N/A

DOCUMENT VERSION

Version: 1.1

COPYRIGHT INFORMATION

© **Copyright 1997 - 2013**, Matrikon Inc. All rights reserved. Apart from any use permitted under the Copyright Act, no part of this manual may be reproduced by any process without the written permission of Matrikon Inc.

CONFIDENTIAL

The information contained herein is confidential and proprietary to Matrikon Inc. It may not be disclosed or transferred, directly or indirectly, to any third party without the explicit written permission of Matrikon Inc.

LIMITATIONS

Matrikon has made its best effort to prepare this manual. Matrikon makes no representation or warranties of any kind with regard to the completeness or accuracy of the contents herein and accepts no liability of any kind including without limitation warranties of merchantable quality, satisfactory quality, merchantability and fitness for a particular purpose on those arising by law, statute, usage of trade, course of dealing or otherwise. Matrikon shall not be liable for any losses or damages of any kind caused or alleged to be caused directly or indirectly from this manual.

LICENSE AGREEMENT

This document and the software described in this document are supplied under a license agreement and may only be used in accordance with the terms of that agreement.

TRADEMARK INFORMATION

The following are either trademarks or registered trademarks of their respective organizations:

MatrikonOPC™ is a division of Matrikon™ Inc. Matrikon and MatrikonOPC are trademarks or registered trademarks of Matrikon Inc.

Adobe, the Adobe logo, Acrobat, the Adobe PDF logo, Distiller and Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Table of Contents

Introduction	6
Who Should Use This Manual	6
<i>Required Software</i>	6
Overview of Manual	6
References	7
Terminology	7
Contacting MatrikonOPC.....	8
DCOM Security Settings.....	9
Additional Security Notes.....	18
Windows Firewall.....	19
User Access Control.....	19
Session 0 Isolation.....	20
Data Execution Prevention	25
Local Security Policy	27
Limitations	35

Table of Figures

Figure 1 My Computer properties – Default Properties settings	9
Figure 2 My Computer Properties – COM Security settings.....	10
Figure 3 Access Permissions dialogue	11
Figure 4 Launch and Activation Permission dialogue.....	12
Figure 5 DCOM Objects List	13
Figure 6 DCOM Settings – General tab.....	14
Figure 7 DCOM Settings – Security Tab	15
Figure 8 DCOM Settings – Endpoints tab	16
Figure 9 DCOM Settings – Identity tab	17
Figure 10 Run dialogue	20
Figure 11 Services panel	21
Figure 12 Properties dialogue	22
Figure 13 Command-line prompt - locating the executable	23
Figure 14 Command-line prompt - registering the program	24
Figure 15 System Properties dialogue	25
Figure 16 Performance Options dialogue	26
Figure 17 Local Security Policy dialogue	27
Figure 18 Machine Access Restrictions dialogue	28
Figure 19 Access Permissions dialogue	29
Figure 20 Local Security Settings - Network Access	30
Figure 21 Network Access - Everyone permissions	31
Figure 22 Network Access: Sharing and security model dialogue.....	32
Figure 23 Local Security Policy - User Rights Assignment	33
Figure 24 Network access properties dialogue	34

Table of Tables

Table 1 - Terms and Definitions..... 7

Table 2 - MatrikonOPC Support Regional Contact Information 8

Introduction

All Classic OPC communication is based on Microsoft COM (Component Object Model) technology. COM defines the rules for creating components within the Microsoft Windows operating system. DCOM (Distributed Component Object Model) is an extension of COM that manages the connection between COM client and COM server software. In managing this connection DCOM performs the marshalling and authentication functions, as well as determining the communication protocol that will be used. In order to achieve successful communication between OPC components, the security of the operating system and the COM components must be properly configured.

The information included in this document will guide you through the process of configuring Windows security to permit maximum connectivity.

Users often experience difficulties with OPC communication on Microsoft Windows 7 and Windows 2008 due to advanced security settings. This document describes how to configure these security settings to allow OPC communication. This document also relates to Microsoft Windows 7 SP1 and Microsoft Windows Server 2008 SP1.



Note: This guide shows you how to enable all DCOM permissions for OPC communications. It is up to the user to disable unused DCOM settings to prevent unauthorized access to their OPC server.

Who Should Use This Manual

This document is intended for all users having difficulties establishing communications between OPC servers, clients, and related applications.


Required Software

This guide has been written and tested for all versions of:

- Microsoft Windows 7 Enterprise
- Microsoft Windows Server 2008
- Microsoft Windows Server 2008 R2

Overview of Manual

This document uses icons to highlight valuable information. Remember these icons and what they mean, as they will assist you throughout the manual.

	<p>This symbol denotes important information that must be acknowledged. Failure to do so may result in the software not functioning properly.</p>
<p>BOLD</p>	<p>Font displayed in this color and style indicates a hyperlink to the applicable/associated information within this manual, or if applicable, any external sources.</p>

This document consists of several sections and is structured as follows:

- **Introduction** – this introductory chapter.
- **DCOM Security Settings** – provides information about setting DCOM permissions to allow communication between DCOM objects.
- **Windows Firewall** – guides you through the steps needed to disable the firewall, if required.

- **User Account Control** – explains how user permissions are restricted, and how to ensure the proper permissions are granted to programs.
- **Session 0 Isolation** – explains how services and applications are isolated from one another, and guides you through the steps to circumvent that if necessary.
- **Data Execution Prevention** – guides you through the steps needed to disable the DEP, if necessary.
- **Local Security Policy** – guides you through the steps needed to establish communication if you are using workgroups.
- **Limitations** – outlines connectivity limitations.

References

This document references information found within the following documents/sites:

- <http://www.matrikonopc.com>
- <http://www.opcsupport.com>
- <http://www.opcfoundation.org>

Terminology

Table 1 provides a list of definitions for terms used throughout this document.

Term/Abbreviation	Description
DCOM	Distributed Component Object Model
DEP	Data Execution Prevention
ACL	Access Control Lists
UAC	User Account Control

Table 1 - Terms and Definitions

Contacting MatrikonOPC

The MatrikonOPC Customer Services department (www.opcsupport.com) is available 24 hours a day, seven days a week.

Contact MatrikonOPC Support using the information below, or send an email (support@MatrikonOPC.com).

For Monday to Friday **daytime support** requests, contact MatrikonOPC Support using the regional phone numbers provided in Table 2.

Region	Office Hours	Contact Information
North America UTC/GMT -7 hours (MST)	8:00 am-5:00 pm	+1-877-OPC-4-ALL
Europe /Africa * UTC/GMT +1 hours (CET)	9:00 am-5:00 pm	+49-221-969-77-0 (Request OPC Support)
Australia/Asia * UTC/GMT +10 hours (AEST)	9:00 am-5:00 pm	+61-2-4908-2198 (Request OPC Support)

* Toll-free regional numbers coming soon!

Table 2 - MatrikonOPC Support Regional Contact Information

DCOM Security Settings

OPC uses ActiveX COM and DCOM to communicate, so we must set the DCOM permissions to allow communication between DCOM objects.

1. Go to **Start -> Run** or use the **Windows Key + R** shortcut to launch the Run window.
2. Type in **dcomcnfg** and click OK.
3. In the **Component Services** window, navigate to **Console Root -> Component Services -> Computers** by clicking on the arrow icons to the left of the headings. Right-click on **My Computer** and select *Properties*.
4. On the **My Computer Properties** window, ensure that the following settings are properly configured:
 - a. On the **Default Properties** tab (Figure 1):
 - i. The **Enable Distributed COM on this computer** option is checked.
 - ii. The **Default Authentication Level** is set to **Connect**.
 - iii. The **Default Impersonation Level** is set to **Identify**. The remaining boxes should remain unchecked unless they were previously configured.

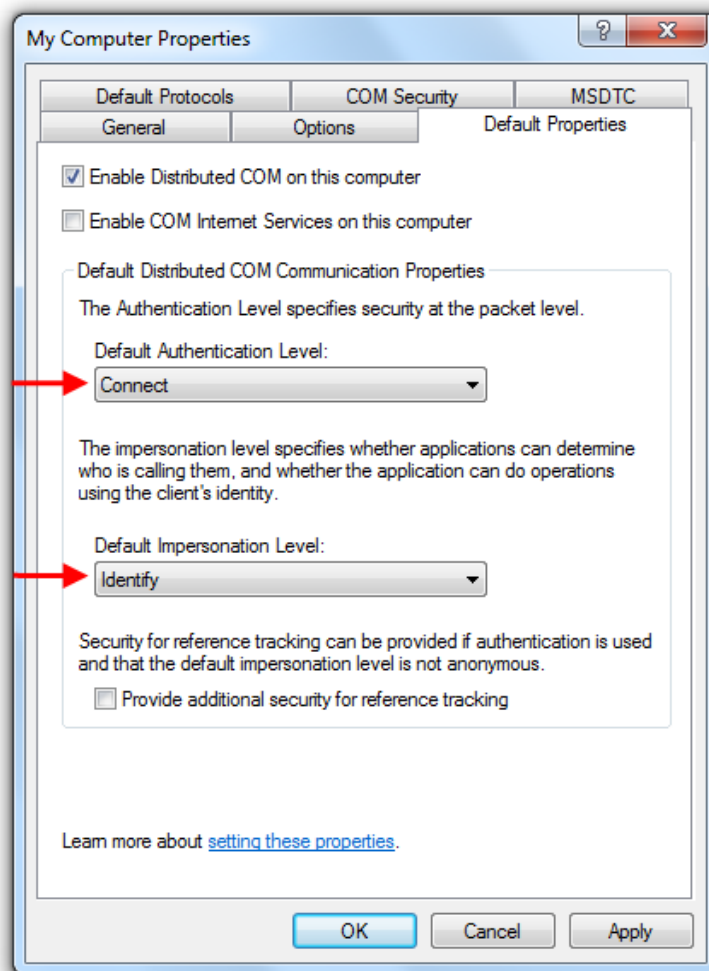


Figure 1 My Computer properties – Default Properties settings

b. On the **COM Security** tab (Figure 2):

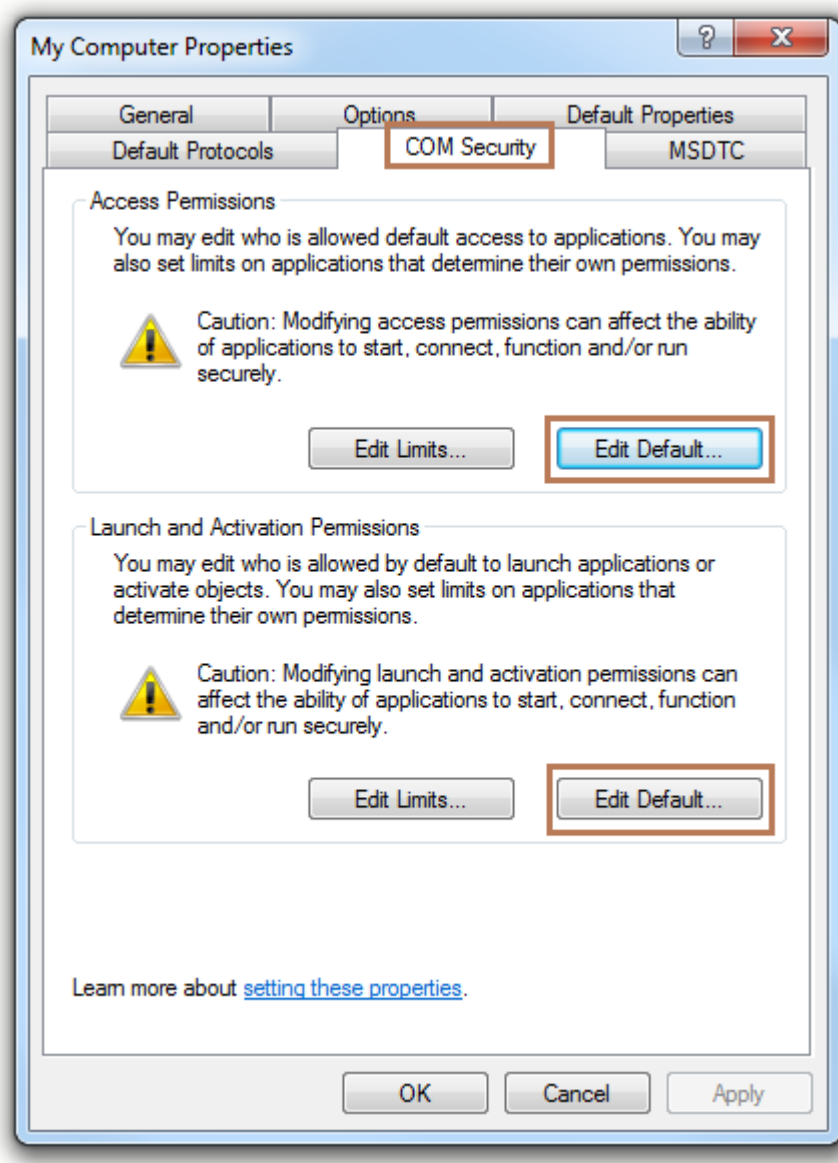


Figure 2 My Computer Properties – COM Security settings

- i. Under **Access Permissions** click on the **Edit Default** button (Figure 3).
- ii. Add the following. Do not remove any others that may already be listed there:
 1. Anonymous Logon (this must be added to the defaults in order for OPC Enumerator to function correctly)
 2. Everyone
 3. Interactive
 4. Network
 5. System
- iii. Ensure that both **Local** and **Remote** Access are **Allowed** for all of the above.
- iv. Click on **OK**.

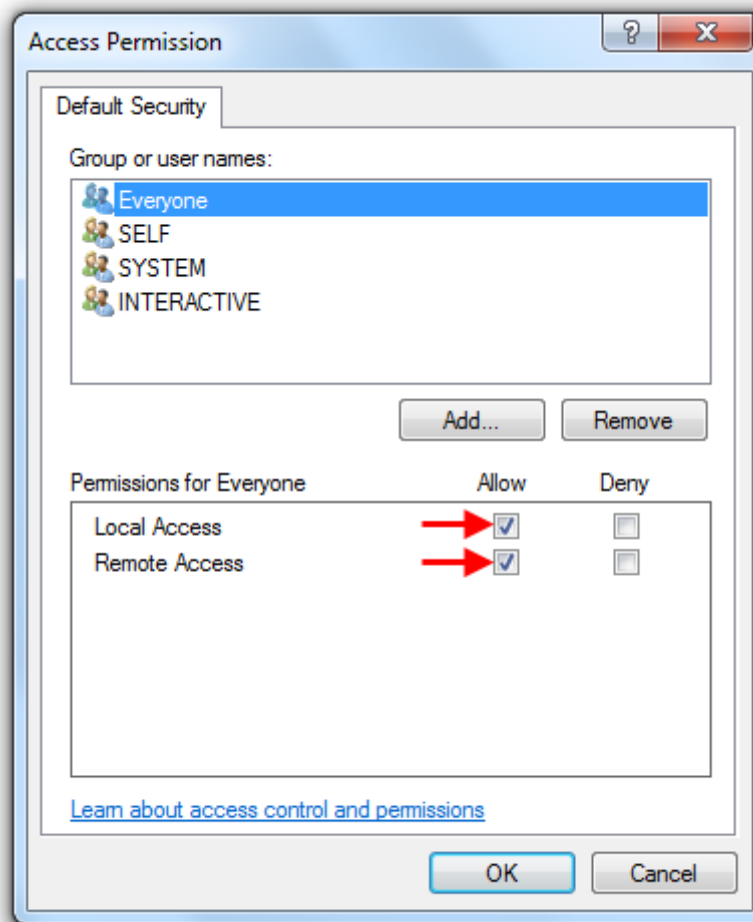


Figure 3 Access Permissions dialogue

- v. Under **Launch and Activation Permissions** (Figure 4) click on the **Edit Default** button.
- vi. Add the following. Do not remove any others that may already be listed there:
 - 1. Anonymous Logon
 - 2. Everyone
 - 3. Interactive
 - 4. Network
 - 5. System
- vii. Ensure that **Local** and **Remote** Launch and Activation are **Allowed**.
- viii. Click on **OK**.

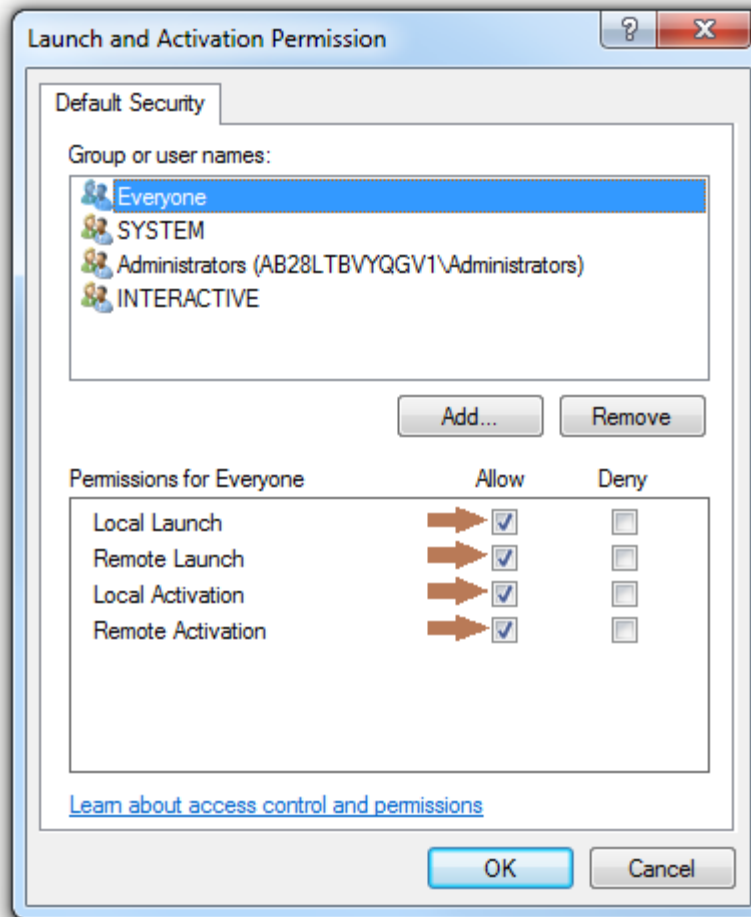


Figure 4 Launch and Activation Permission dialogue

- a. The **Edit Limits** (Figure 2) option in this tab applies machine-wide settings for **Access** and **Launch** permissions. These settings are the same as the DCOM options in the Local Security Policy, but are recorded in different Registry keys. Due to the fact that Windows applies Local Security Policies with a higher priority than the Registry keys applied by these settings, when the Local Security Policy Options for these configuration items are set, the **Edit Limits** buttons will be greyed out or *inactive*.

When configuring the DCOM settings for your computer, if the Edit Limits buttons are active, do not make changes here. The procedure for configuring the Local Security Policy Options will negate these changes, and will be covered later in this document.



Note: Recent Microsoft Windows updates have changed this setting. If your system has been updated to the latest level, all security and update patches applied, you must configure both the Local Security Policy options described later in this document and these machine-wide Limits settings.

5. The DCOM settings for each OPC Server object must now be individually configured. This serves two (2) purposes:
 - a. It removes dependence on the Default settings for each server, and
 - b. It allows for permissions on each Server object to be restricted to only those who require it.
6. Under **My Computer**, open the folder labeled **DCOM Config** (Figure 5).

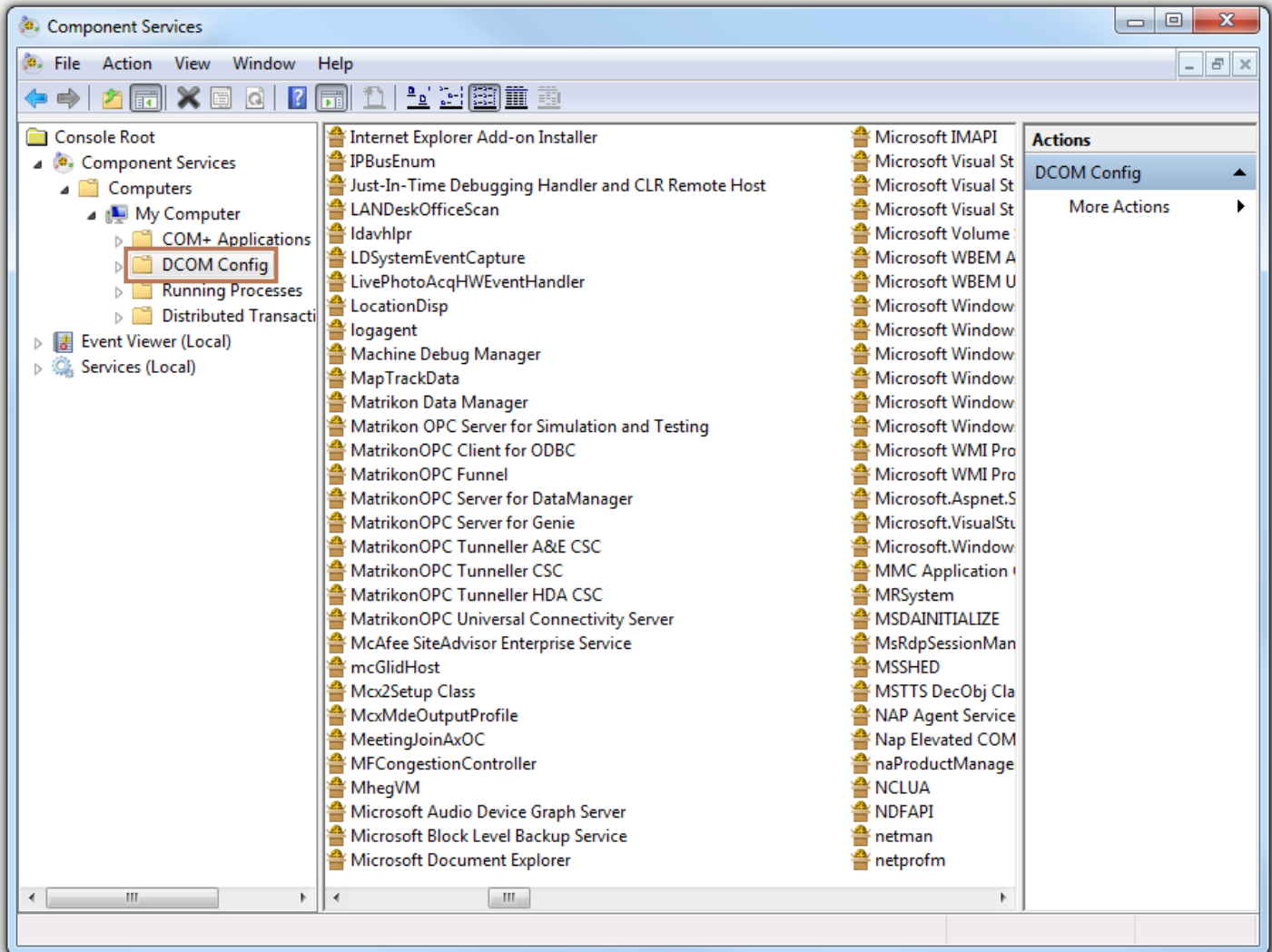


Figure 5 DCOM Objects List

7. To edit the settings for each OPC Server, browse to the OPC Server, right-click on it, and select **Properties**.

- a. On the **General** tab (Figure 6), set the Authentication Level to **Connect**.

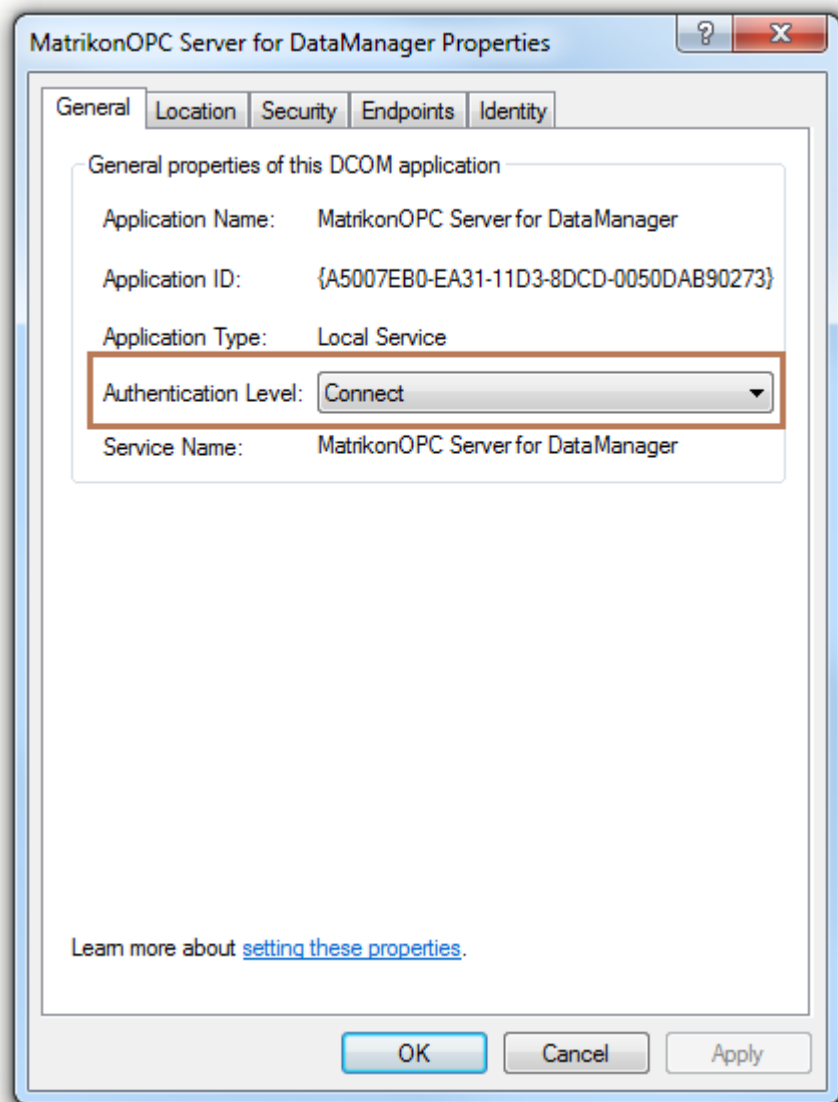


Figure 6 DCOM Settings – General tab

- b. On the **Security** tab (Figure 7):
 - i. Under **Launch and Activation Permissions**, select the Customize radio button. Then click on Edit.

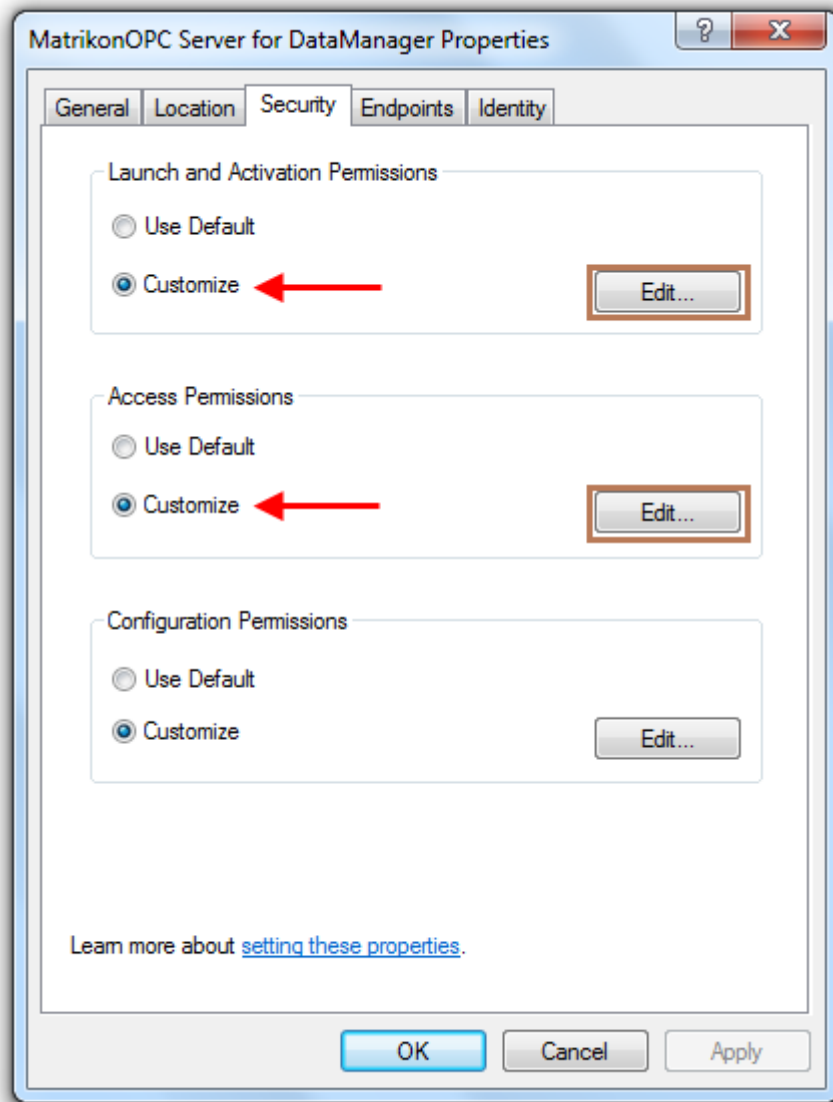


Figure 7 DCOM Settings – Security Tab

- ii. Add the following users:
 1. Everyone
 2. Interactive
 3. Network, and
 4. System. Anonymous Logon is not necessary for this permissions field.
- iii. Ensure that all Users have **Local** and **Remote**, **Launch** and **Activation** permissions *Allowed* selected. Then click **OK**.

- iv. Under **Access Permissions** select the **Customize** radio button. Then click **Edit**.
 - v. Add the following users:
 1. Everyone
 2. Interactive
 3. Network, and
 4. System. Anonymous Logon is not necessary for this permissions field.
 - vi. Ensure that all Users have **Local** and **Remote** Access permissions *Allowed* selected. Then click **OK**.
- c. On the **Endpoints** tab (Figure 8), ensure that *Connection-oriented TCP/IP* is entered in the list. To add this option, click the **Add** button, select *Connection-oriented TCP/IP* in the dropdown list, and ensure the **Use default endpoints** radio button is selected.

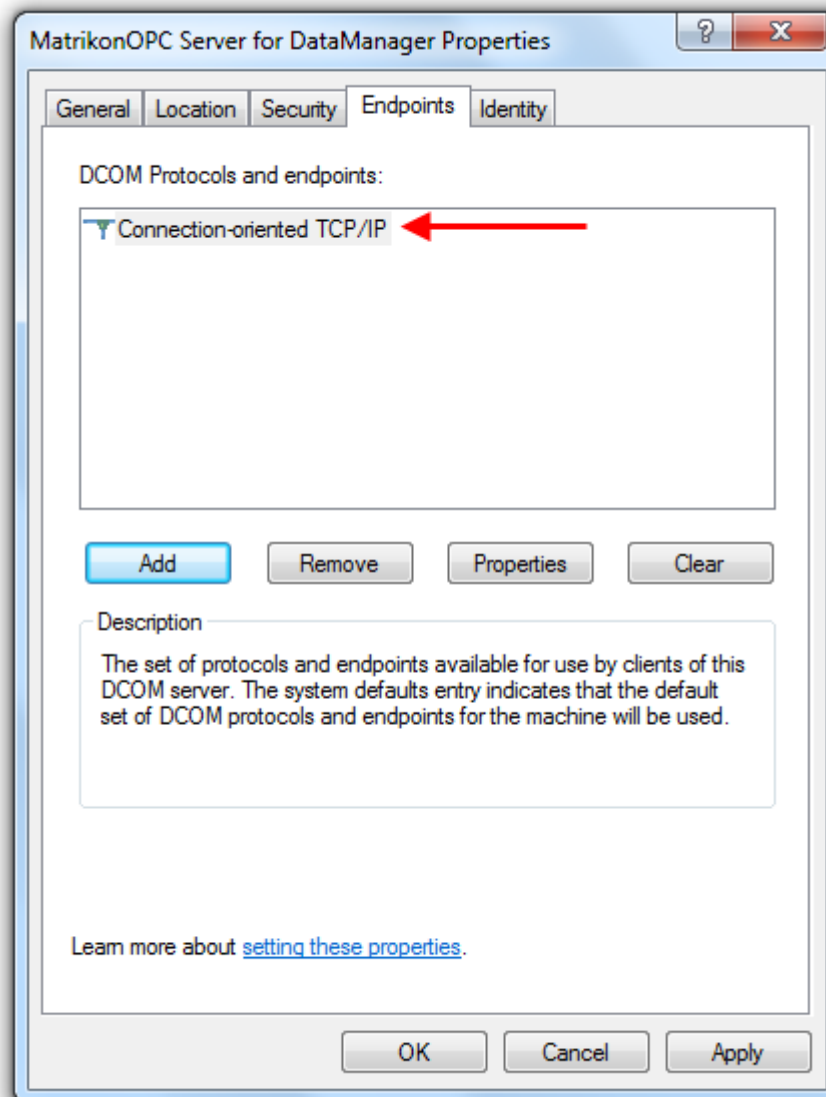


Figure 8 DCOM Settings – Endpoints tab

- d. On the **Identity** tab (Figure 9), ensure that your server is running either **System account** (recommended if the object is running as a service) or **This user** (recommended if the object is running as an application); if **This user** is selected, please enter the username and password of a user account with full Administrator permissions. It is highly recommended that the **Launching User** identity not be used. Click **OK** to return to the **Component Services** window.

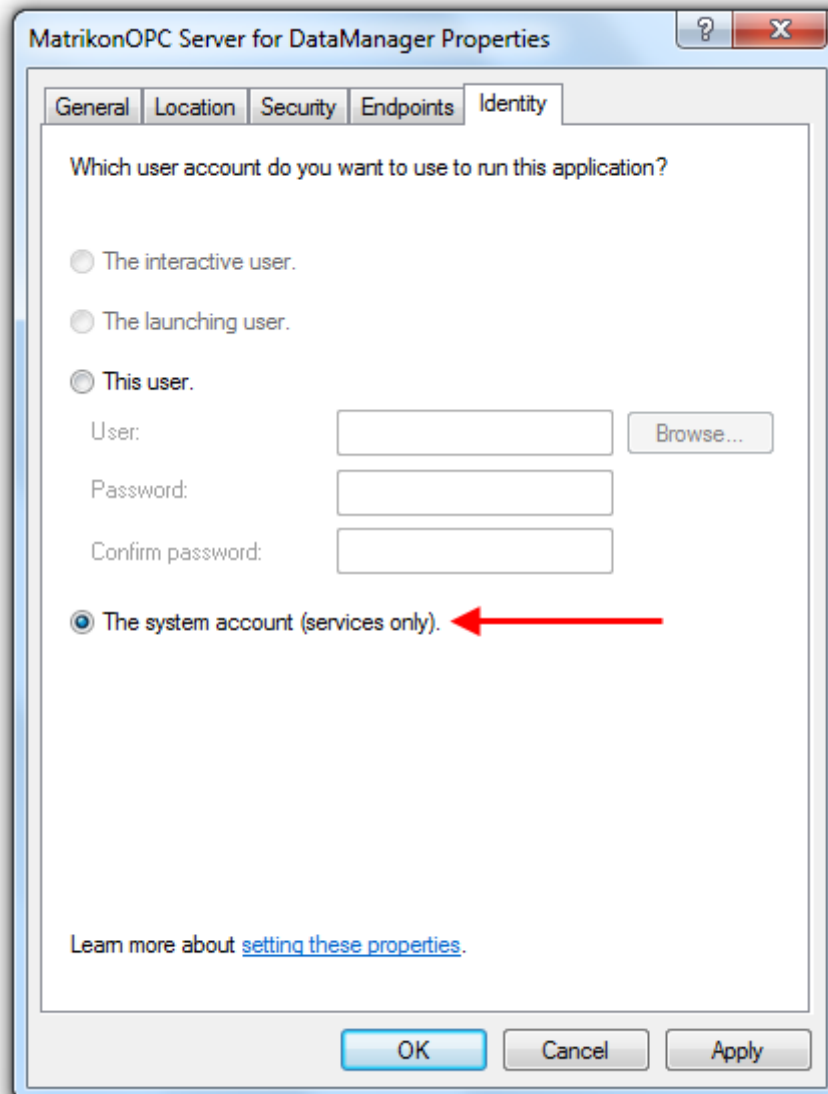


Figure 9 DCOM Settings – Identity tab



Additional Security Notes

By setting the Identity to **Interactive User** it is necessary to remain logged on at this computer in order for the application to run. This may represent a contradiction of your Company IT Security Policy. If this software must be run as an application, it may be more effective to run as **This user** and provide credentials for the application to use.

In order for the OPC server objects to be properly discovered by OPC clients, the OPC Server List Utility, OPC Enumerator, must also be properly configured for DCOM. This utility is a COM server and must allow connection and access by the clients as well.

Windows Firewall

For Windows 7 and Windows Server 2008, the Windows Firewall is turned on by default. This software firewall will prevent DCOM communication by blocking the remote calls that DCOM requires for such functions as DNS name resolution, function calls and callbacks, to name a few. Exceptions can be made in the firewall, either by application or by port number. This process is described elsewhere, for example in the Windows Help files. The issue is that DCOM requires such a wide range of ports be opened that there are serious gaps left in the security of the system thus configured.

It is more effective to turn the firewall off, if permitted by your company IT policy. If not permitted, contact your IT department and request permission to temporarily turn it off in order to troubleshoot the system. To turn off the Windows Firewall, follow this procedure:

1. Go to **Start -> Control Panel**.
2. Double-click the **Windows Firewall** icon.
3. Select **Turn Windows Firewall on or off** on the left side of the window.
4. For the appropriate network location (generally the Domain network location settings), select the Turn off Windows Firewall radio button.

User Access Control

In order to heighten security, an access list-based security measure known as User Access Control (UAC) was implemented in Windows 7 and Server 2008. UAC limits the permissions granted to users by default to a non-administrative user; in order to perform administrator tasks (such as accessing protected parts of the filesystem), the user's permissions can be temporarily elevated.

To force a permission elevation, you can right-click on an icon and choose "Run As Administrator"; if the launching user is not part of the Administrators group you will be prompted for administrator credentials.

As MatrikonOPC products require access to protected parts of the filesystem to perform certain tasks, we strongly recommend using Run As Administrator to license MatrikonOPC software and run MatrikonOPC configuration utilities. The MatrikonOPC servers themselves should not be affected by User Account Control, as they do not need to modify the registry.

Session 0 Isolation

In previous versions of Windows, all services ran in the first session on the machine (Session 0), and the first user who logs on to the system will log into that same session. As this practice poses a security risk, session 0 was isolated in Windows 7 and Windows Server 2008; the first user will now log into session 1, second user into session 2, et cetera. DCOM communication can take place over session boundaries (and therefore OPC communication); however Session 0 isolation can interfere with DDE communications (eg. Passing data to/from Excel – a DDE server), as well as other protocols an OPC server uses that may depend on 3rd party APIs.

As a general guideline, if you have an OPC client set to run as an application (and therefore as a given user), any local OPC client (which may include the server-side component of OPC tunneling software) should be running as the same user.

To register a MatrikonOPC program as an application:

1. Open the **Run** dialogue (**Start -> Run...**) and enter **services.msc** (Figure 10). Click **OK**.

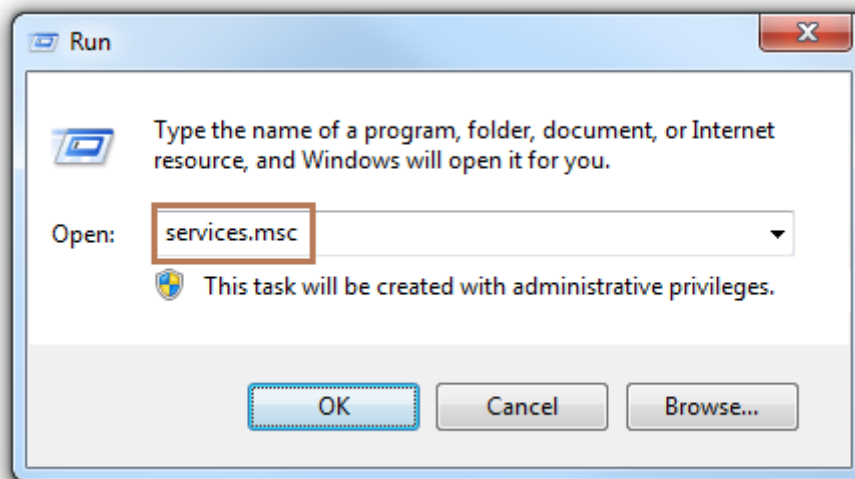


Figure 10 Run dialogue

2. Locate the program in the Services panel (Figure 11). If the Status is listed as Started, right-click the server and select Properties. If not, please skip to step 5.

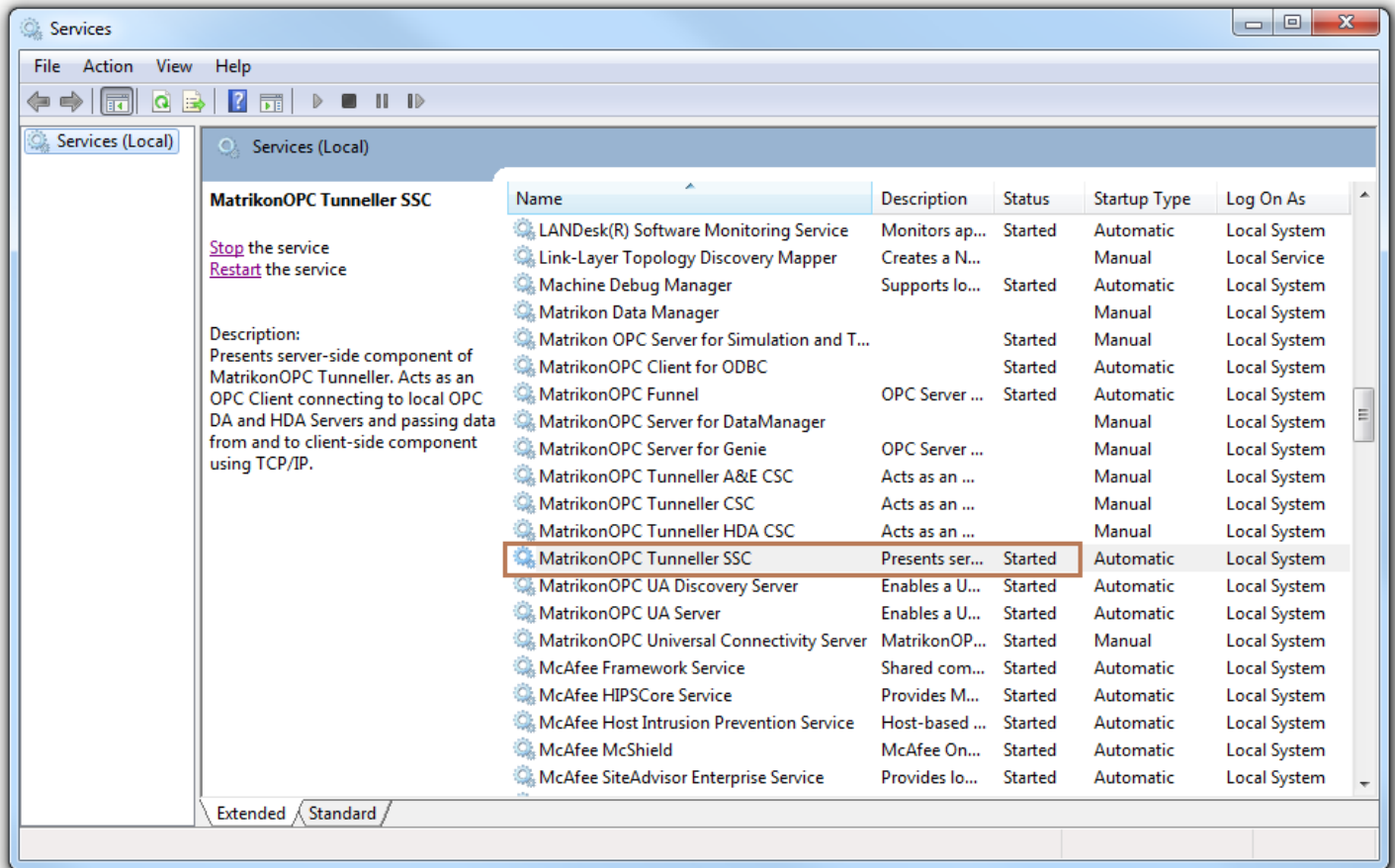


Figure 11 Services panel

3. In the Properties dialogue (Figure 12) under the General tab, set the Startup type to Disabled and click the Stop button under Service status. Click OK.

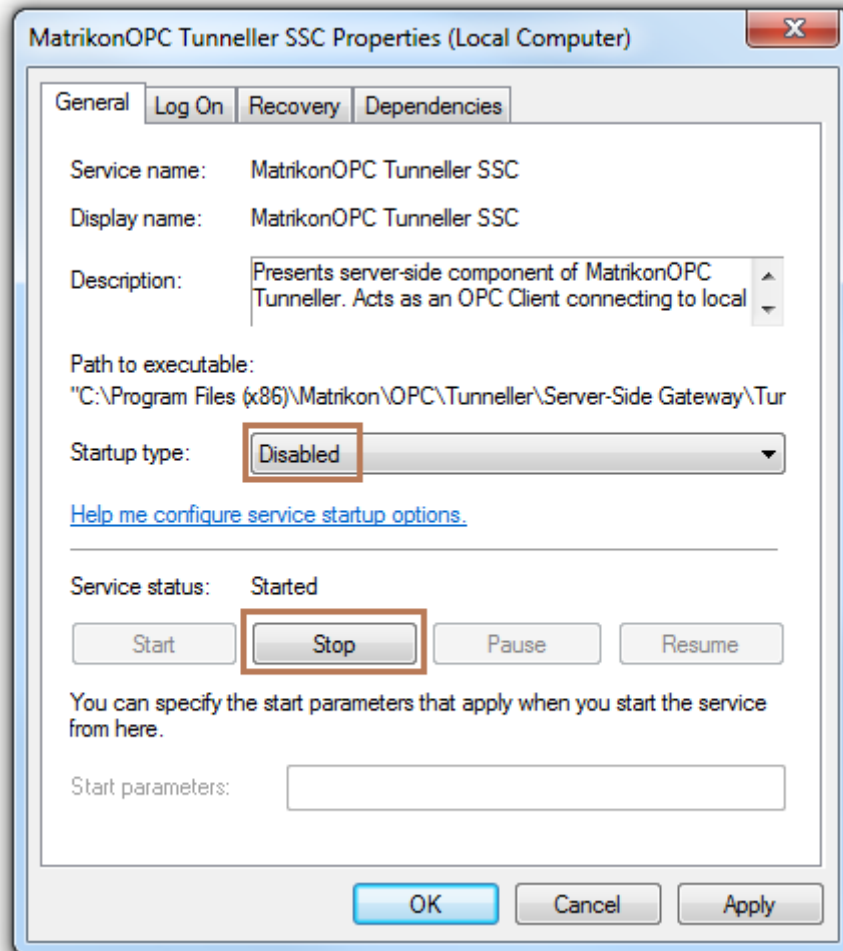
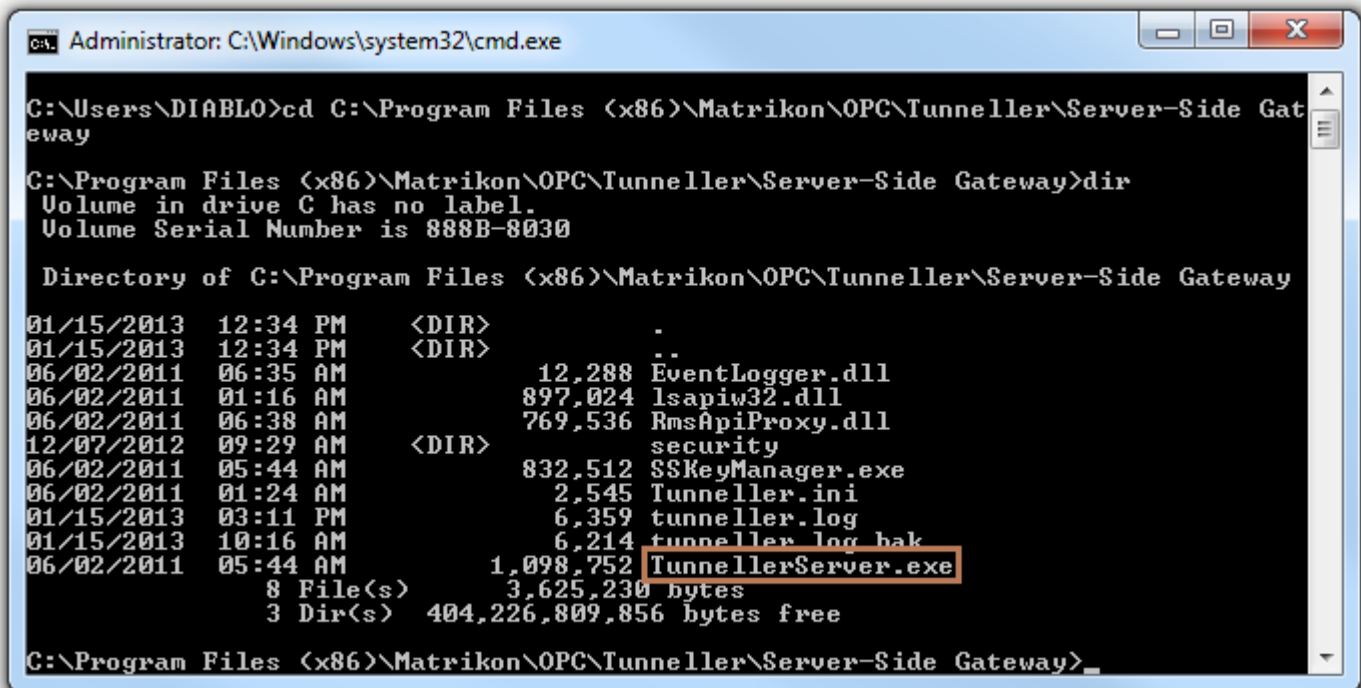


Figure 12 Properties dialogue

4. The service should no longer be listed as Started, and the Startup Type should now read Disabled. If this is not the case, please repeat step 3.

- Open a command-line prompt (Start -> Run... "cmd.exe", no quotes) and navigate to the directory containing the program's executable file (Figure 13).



```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\DIABLO>cd C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway

C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway>dir
Volume in drive C has no label.
Volume Serial Number is 888B-8030

Directory of C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway

01/15/2013  12:34 PM    <DIR>          .
01/15/2013  12:34 PM    <DIR>          ..
06/02/2011  06:35 AM             12,288 EventLogger.dll
06/02/2011  01:16 AM             897,024 lsapiw32.dll
06/02/2011  06:38 AM             769,536 RmsApiProxy.dll
12/07/2012  09:29 AM    <DIR>          security
06/02/2011  05:44 AM             832,512 SSKeyManager.exe
06/02/2011  01:24 AM              2,545 Tunneller.ini
01/15/2013  03:11 PM              6,359 tunneller.log
01/15/2013  10:16 AM              6,214 tunneller_log_bak
06/02/2011  05:44 AM             1,098,752 TunnellerServer.exe
               8 File(s)              3,625,230 bytes
               3 Dir(s)  404,226,809,856 bytes free

C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway>_
  
```

Figure 13 Command-line prompt - locating the executable

- Type in [filename.exe] -unregserver. This will unregister the program.
- To register the program as an application, type in [filename.exe] -regserver (Figure 14).
- To register the program as a service, type in [filename.exe] -service.

```

Administrator: C:\Windows\system32\cmd.exe

01/15/2013 12:34 PM <DIR> .
01/15/2013 12:34 PM <DIR> ..
06/02/2011 06:35 AM      12,288 EventLogger.dll
06/02/2011 01:16 AM    897,024 Isapiw32.dll
06/02/2011 06:38 AM    769,536 RmsApiProxy.dll
12/07/2012 09:29 AM <DIR> security
06/02/2011 05:44 AM    832,512 SSKeyManager.exe
06/02/2011 01:24 AM      2,545 Tunneller.ini
01/15/2013 03:11 PM      6,359 tunneller.log
01/15/2013 10:16 AM      6,214 tunneller.log.bak
06/02/2011 05:44 AM    1,098,752 TunnellerServer.exe
      8 File(s)      3,625,230 bytes
      3 Dir(s)  404,226,809,856 bytes free

C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway>TunnellerServe
r.exe -unregserver

C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway>TunnellerServe
r.exe -regserver

C:\Program Files (x86)\Matrikon\OPC\Tunneller\Server-Side Gateway>

```

Figure 14 Command-line prompt - registering the program

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 Windows 7 and Windows Server 2008, DEP is enforced by hardware and software.

DEP will also prevent many installations from running, and has been known to cause other software issues. Most MatrikonOPC software released since late 2006 will detect the DEP setting and, if turned on, terminate the installation process.



Most MatrikonOPC software released since August 2009 no longer requires DEP to be turned off. Please verify this by reading the release notes and user manual for each application installed.

If the software has been installed with DEP turned on, the following steps must be performed:

1. Turn DEP *OFF*.
2. Restart the Operating System.
3. Uninstall the OPC software.
4. Reinstall the OPC software.

To turn DEP *OFF*, perform the following steps:

1. From your Start menu, right-click on **Computer** and select **Properties**.
2. On the Advanced tab (Figure 15), under Performance, click the Settings button.

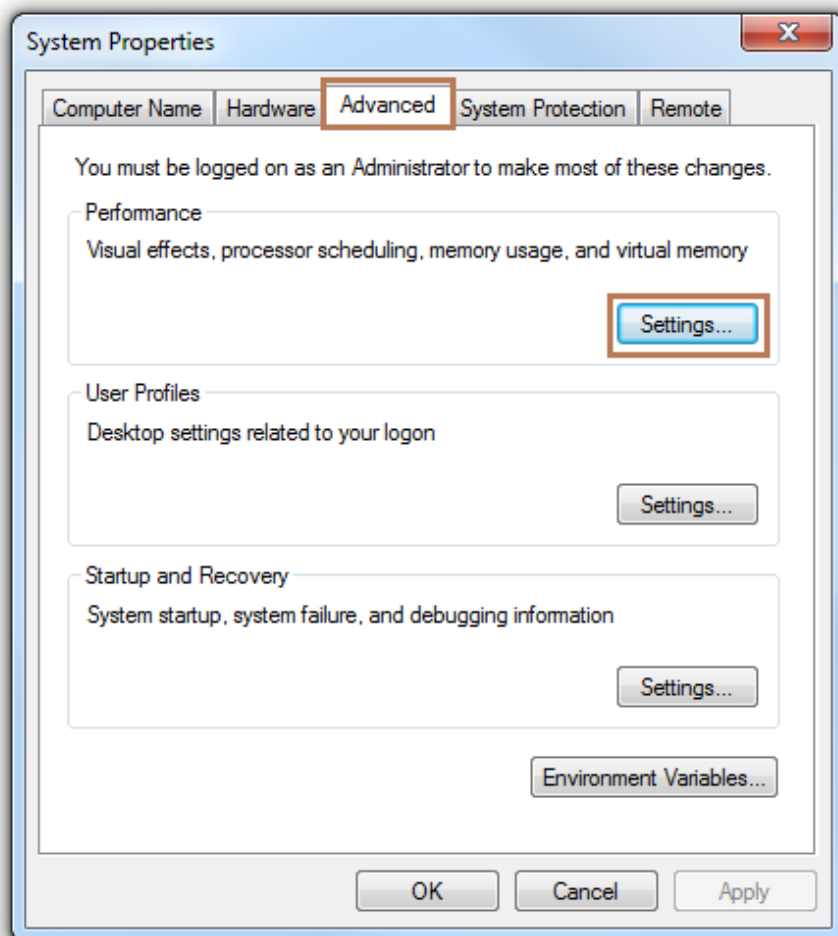


Figure 15 System Properties dialogue

3. In the **Performance Options** dialogue, on the **Data Execution Prevention** tab (Figure 16), select the **Turn on DEP for essential Windows programs and services only** option. This is the setting we refer to as *OFF*.

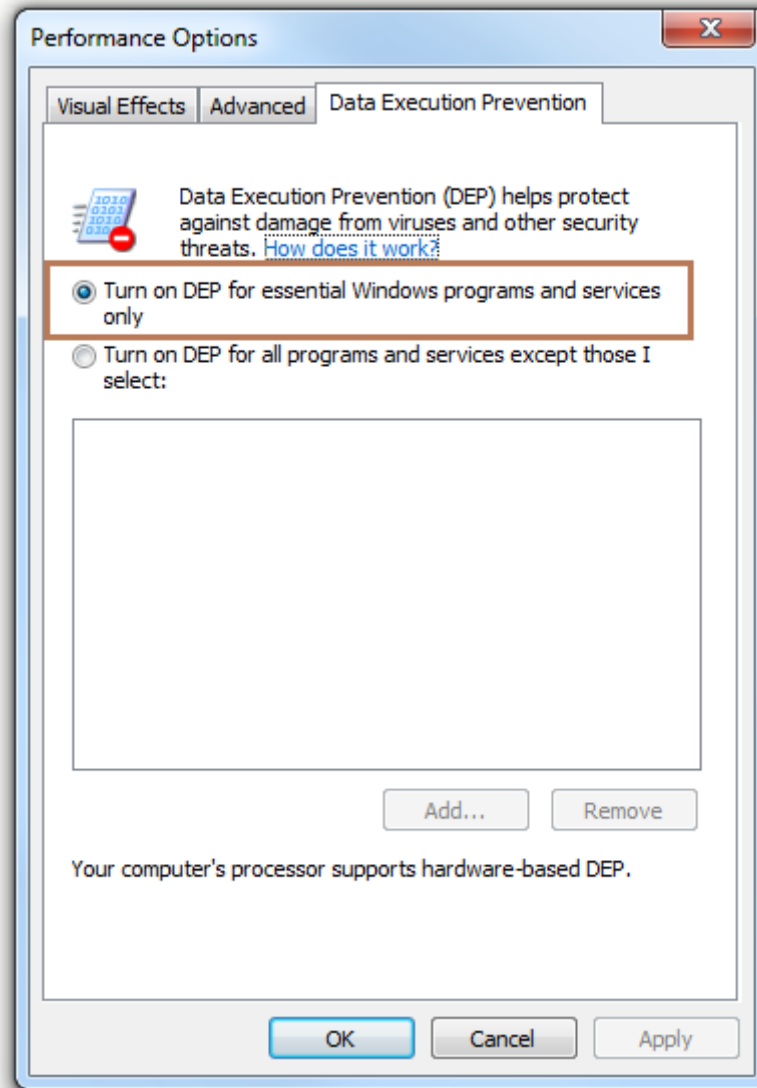


Figure 16 Performance Options dialogue

4. Click **OK**. If you changed the setting, it will be necessary to restart the operating system.

Local Security Policy

If you are using workgroups instead of domains the following steps may need to be taken in order to establish communication. Please note these changes may compromise the security of your system – speak with your network administrator if you have any concerns.

1. Navigate to **Start -> Control Panel -> Administrative Tools -> Local Security Policy**.
2. Navigate to **Security Settings -> Local Policies -> Security Options** (Figure 17).
3. Right-click on **DCOM: Machine Access Restrictions...** and select **Properties**, or double-click on this option. Either method will open the **Properties** dialogue.

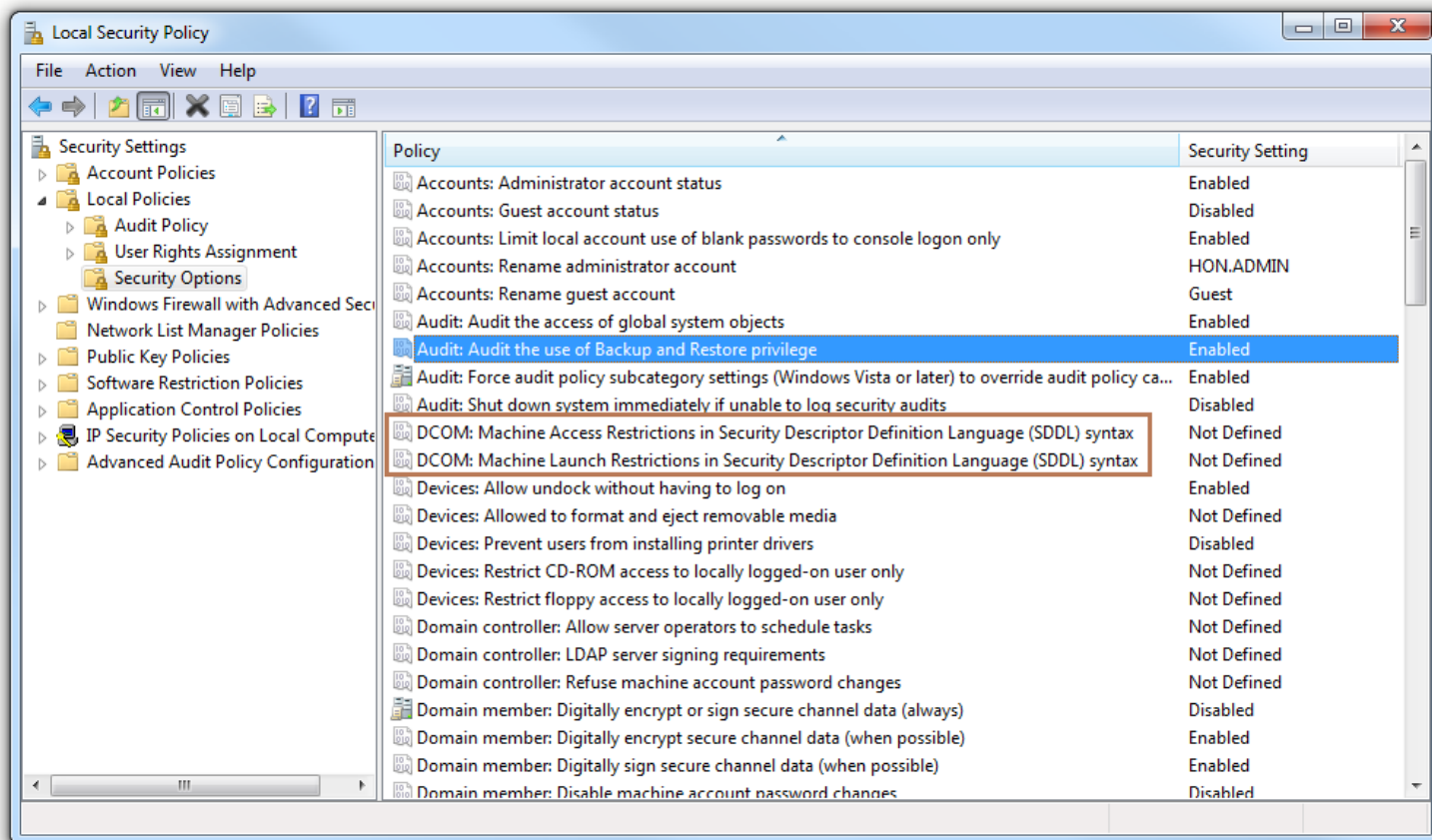


Figure 17 Local Security Policy dialogue

4. Click on the **Edit Security** button.

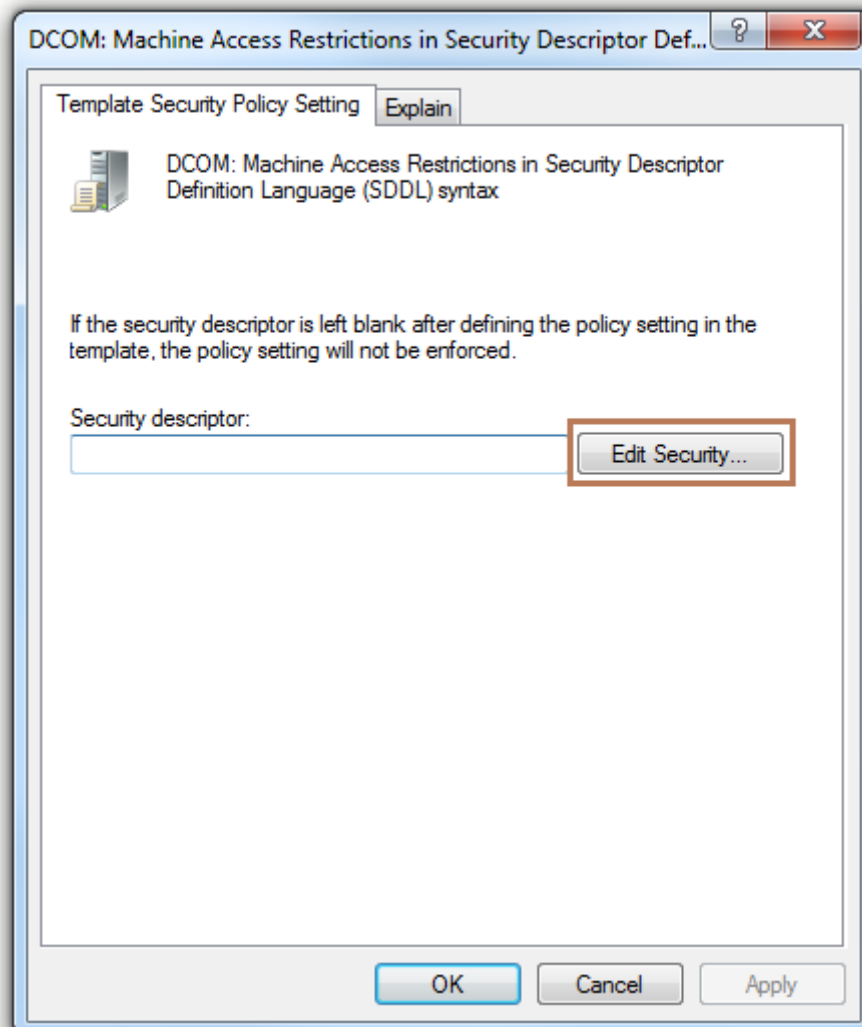


Figure 18 Machine Access Restrictions dialogue

- a. Ensure that the following Users/Groups are added and that all have **Local** and **Remote** access allowed (this is the same as the Access permission configuration in the Default DCOM settings):
 - i. Anonymous Logon
 - ii. Everyone
 - iii. Interactive
 - iv. Network, and
 - v. System
- b. Click **OK** to return to the main security policy window.

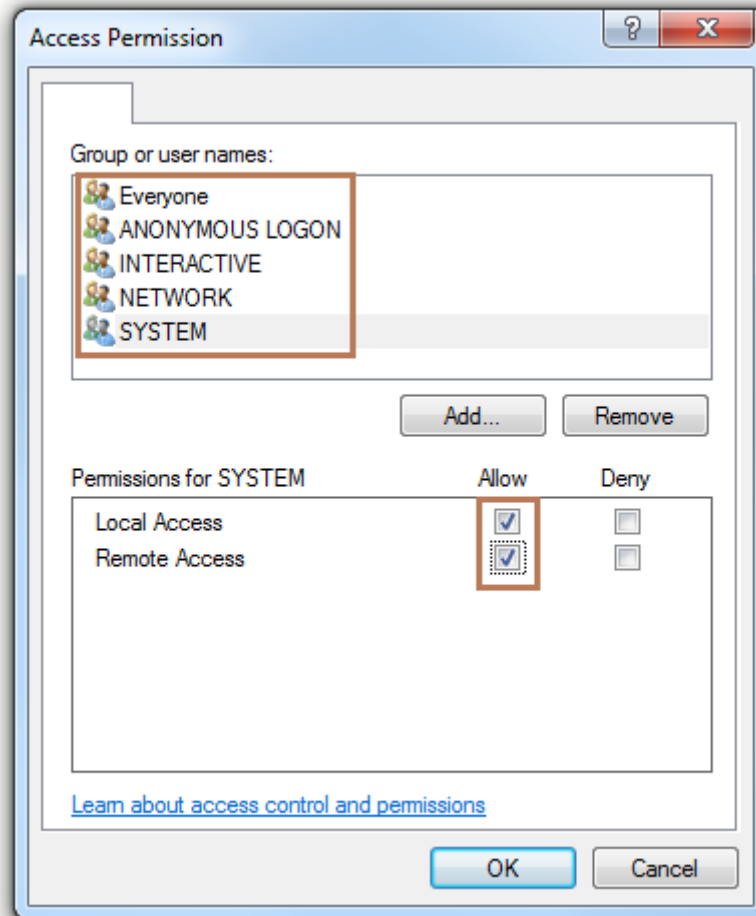


Figure 19 Access Permissions dialogue

5. Repeat this process for the **DCOM: Machine Launch Restrictions...** settings.



Note: These settings will supersede the Limits settings in the Default DCOM Settings, as described in paragraph 4c of the previous section. Please refer to the note on that section for relevance of Windows Update status to these settings and those of the Machine-Wide Limits.

- Return to the Local Security Policy Options and select the **Network Access: Let Everyone permissions apply to anonymous users** (Figure 20).

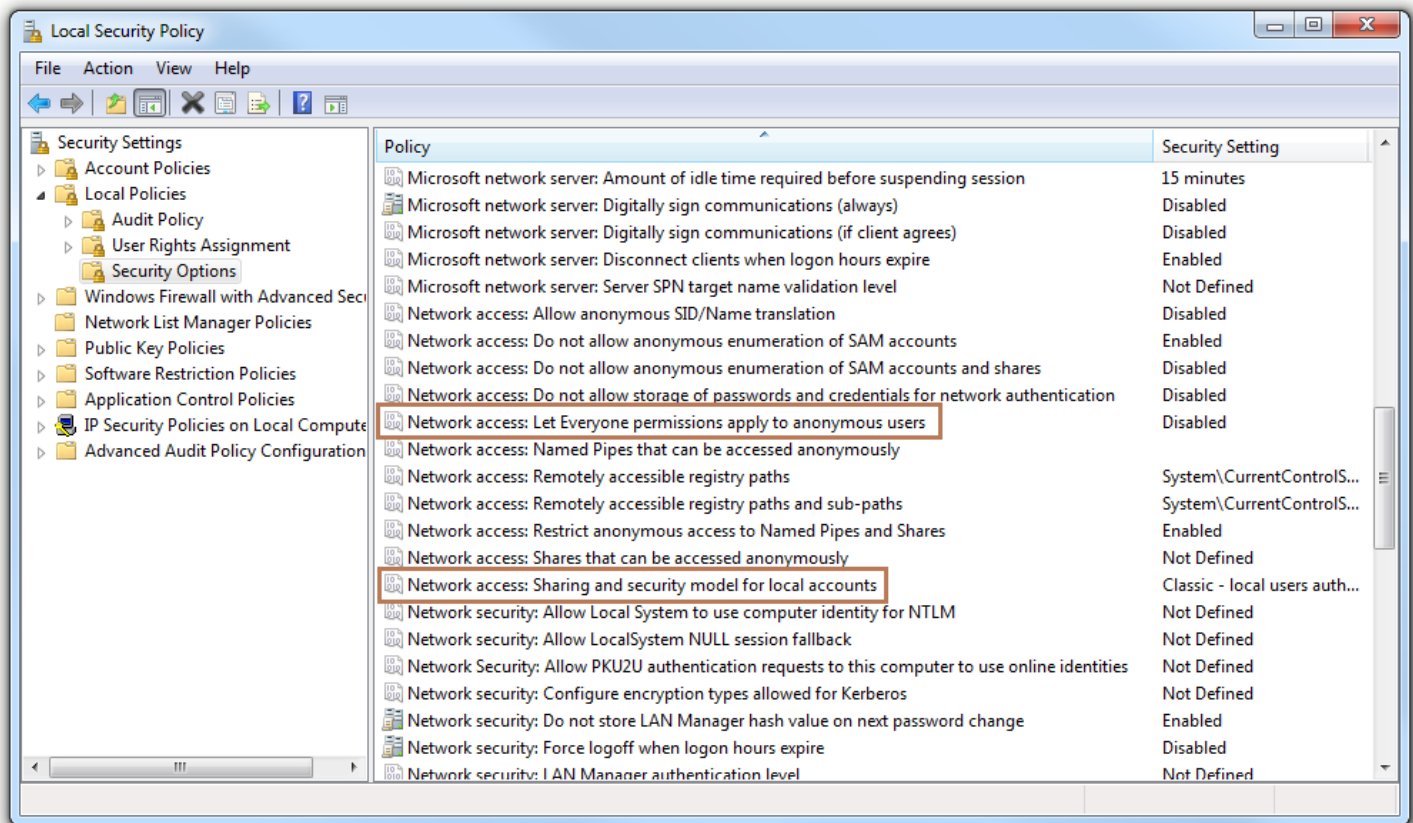


Figure 20 Local Security Settings - Network Access

7. Double-click the setting to open the dialogue (Figure 21), and select **Enable**.

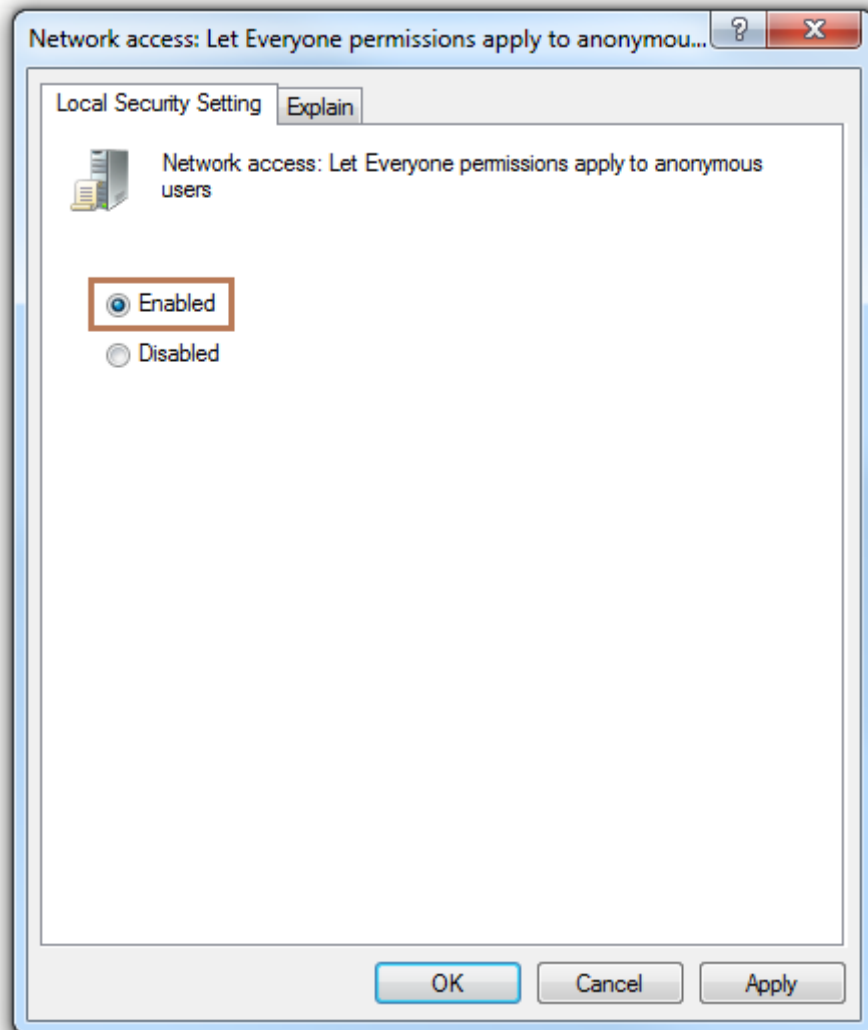


Figure 21 Network Access - Everyone permissions

8. Return to the Local Security Policy Options and select the **Network Access: Sharing and security model for local users**.

9. Double-click the setting to open the dialogue (Figure 22), and select the **Classic – local users authenticate as themselves** option from the drop-down menu.

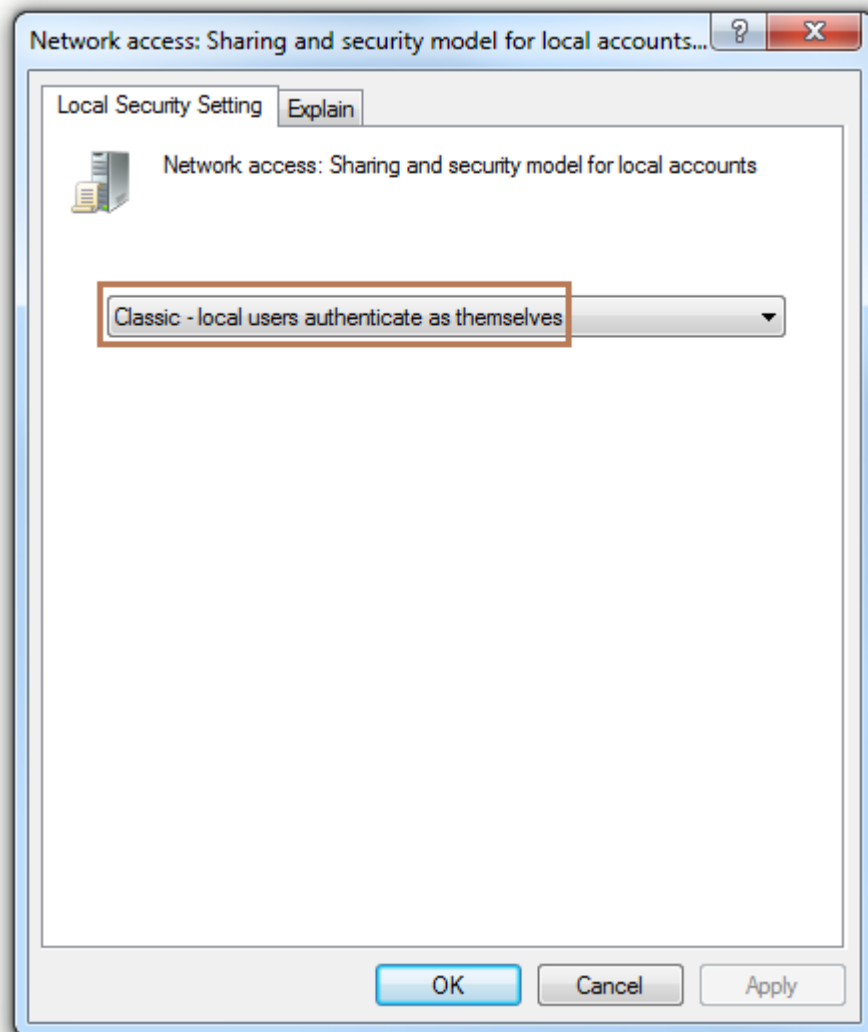


Figure 22 Network Access: Sharing and security model dialogue

10. Return to the Local Security Policy settings and select **User Rights Assignment** from the **Local Policies** group. Double-click on the **Access this computer from the network** to open the dialog for this setting.

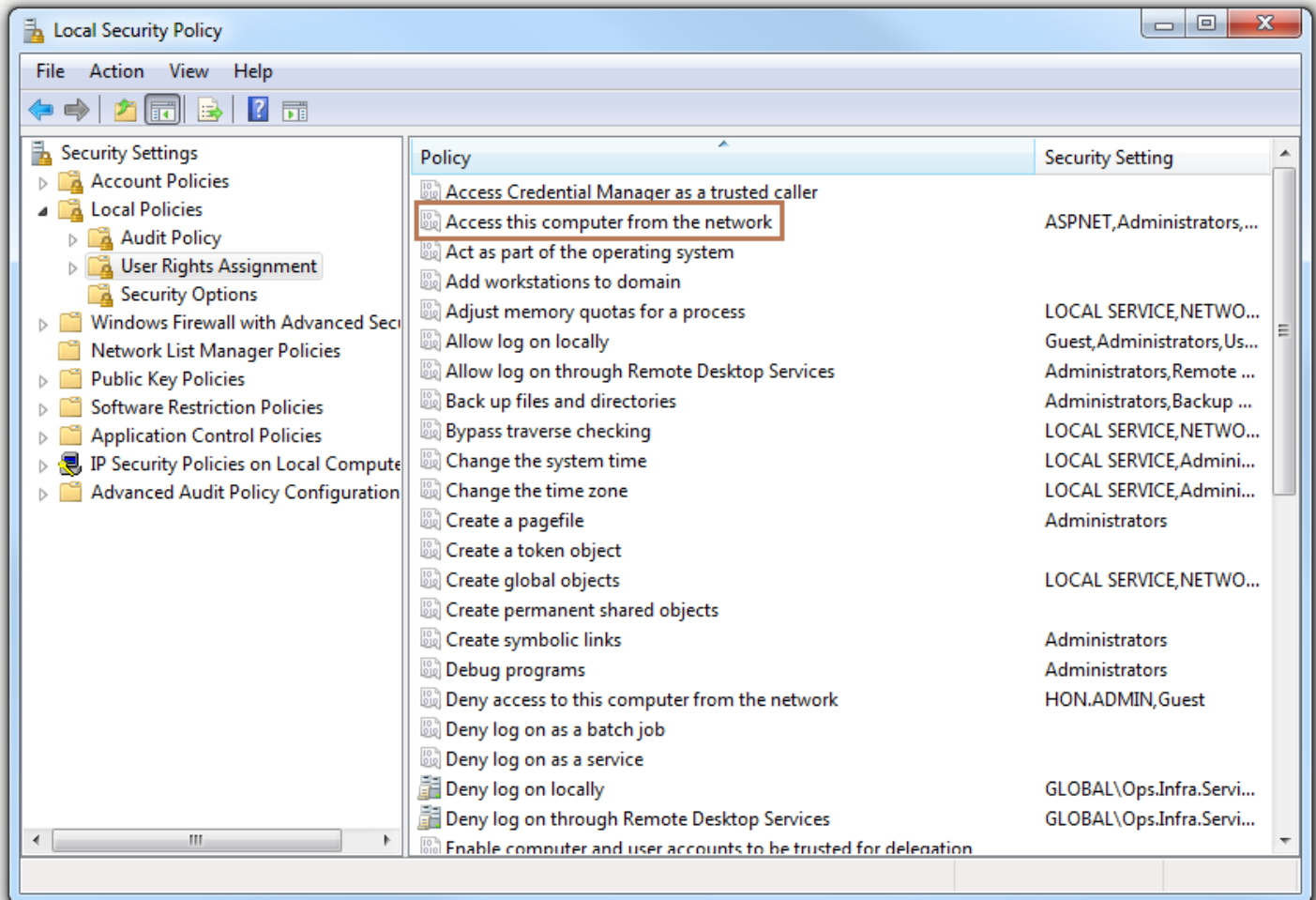


Figure 23 Local Security Policy - User Rights Assignment

11. Ensure the Everyone and Users entries are added to this setting to allow access from the network. Do not remove any entries already present.

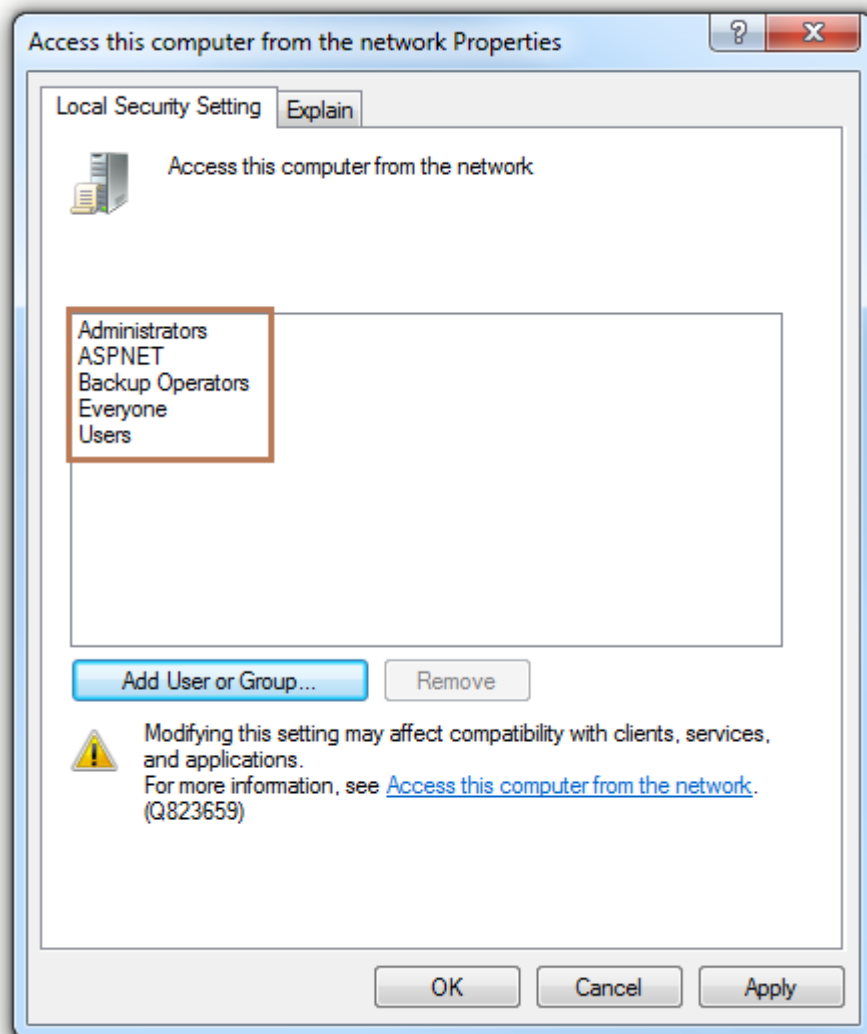


Figure 24 Network access properties dialogue

12. Your DCOM is now set up to accept all incoming connections.

Notes

- These settings will allow full access to your system. This is required to ensure connectivity.
- The security on your system has been set to its lowest state.
- Further configuration will be required to ensure that the security of your system meets with your company's Security and IT policies.

Limitations

DCOM was developed to function in a specific environment where the following conditions applied:

1. All machines and users belonged to the same domain.
2. There were no firewalls enabled on any machines or network devices.
3. All communication media were highly reliable.
4. There were no bandwidth restrictions.

All of these were typical of a LAN setup in an average office environment; however this bears little resemblance to the process control networks of today. Multiple domains, security-oriented IT policies, geographically-dispersed data sources, and a multitude of other factors all make OPC communication based on DCOM extremely complicated to configure while maintaining security.

Tunnelling technology can provide successful OPC communications across firewalls or domain/workgroup barriers. Using a single TCP port to the remote computer, issues involving workgroups, domains, and firewalls no longer hamper OPC communication. This allows you to establish OPC communication without sacrificing security.

The MatrikonOPC Tunneller is one of our most popular products because of its ease of use, automatic reconnection system, and time savings in implementation that it offers. Contact your Account Manager or visit our website at www.matrikonopc.com for more information on this and other MatrikonOPC solutions.