

Head Office Edmonton, AB, Canada Suite 1800 10405 Jasper Avenue T5J 3N4

Main: +1-780-448-1010 Fax: +1-780-448-9191 www.matrikonopc.com

OPC Support:

+1-877-OPC-4-ALL +1-780-945-4011 support@matrikonopc.com www.opcsupport.com

OPC Sales: +1-780-945-4099 drivers@matrikonopc.com

OPC Training: +1-780-945-4011 training@matrikonopc.com www.opctraining.com

Regional Offices

Texas/Louisiana +1-713-490-3737 houstonopc@matrikonopc.com

Germany +49-221-96977-0 europe@matrikonopc.com

Australia +61-8-9315-0100 asiapacific@matrikonopc.com

United Kingdom +44-1629-580886 uk@matrikonopc.com

Middle East +973-3996-9393 middle-east@matrikonopc.com

Establishing OPC Communication on Windows XP SP2 and Windows 2003 SP1

Users will often experience difficulties with OPC Communication on Windows XP SP2 and Windows 2003 SP1 due to advanced security settings. This document describes how to disable these security settings to allow OPC Communication.

DCOM Security Settings

OPC uses ActiveX COM and DCOM to communicate, so we must open our DCOM permissions to allow this.

1. Go to 'Start->Run'





2. Type in 'dcomcnfg' and click OK.

Head Office Edmonton, AB, Canada Suite 1800 10405 Jasper Avenue T5J 3N4

Main: +1-780-448-1010 Fax: +1-780-448-9191 www.matrikonopc.com

OPC Support:

+1-877-OPC-4-ALL +1-780-945-4011 support@matrikonopc.com www.opcsupport.com

OPC Sales: +1-780-945-4099 drivers@matrikonopc.com

OPC Training: +1-780-945-4011 training@matrikonopc.com www.opctraining.com

Regional Offices

Texas/Louisiana +1-713-490-3737 houstonopc@matrikonopc.com

Germany +49-221-96977-0 europe@matrikonopc.com

Australia +61-8-9315-0100 asiapacific@matrikonopc.com

United Kingdom +44-1629-580886 uk@matrikonopc.com

Middle East +973-3996-9393 middle-east@matrikonopc.com

Run	? 🔀
-	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.
Open:	dcomcnfg 🛛 🗸
	OK Cancel Browse

3. Go to 'Console Root->Component Services->Computers->My Computer'. Right-click on 'My Computer' and select 'Properties'.

Scomponent Services		
纋 File Action View W	indow Help	_ 8 ×
← → 🛍 🖬 😰	😫 🎦 🔚 🏗 🏢 🎆 🚇	
Console Root	Component Services 1 object(s)	
Component Services		
🛨 🔝 Event Viewer (Local)	Stop MS DTC	
⊕ 🎇 Services (Local)	Refresh all components	
	New Window from Here	
	Properties	
	Help	
Opens property sheet for the c	urrent selection.	

4. Go to the 'Default Properties' tab and ensure that your Window matches the one shown below:

My Computer Properties		? 🛛
Default Protocols	MSDTC	COM Security
General	Options	Default Properties
Enable Distributed COM	on this computer	
Enable COM Internet Se	rvices on this com	puter
- Default Distributed COM C	Communication Pro	perties
The Authentication Level	specifies security a	at the packet level.
Default Authentication L	.evel:	
Connect		•
The impersonation level sp who is calling them, and w using the client's identity.	pecifies whether a whether the application	pplications can determine tion can do operations
Default <u>Impersonation</u> L	evel:	
Identify		▼
Security for reference trac and that the default imper <u>Provide</u> additional se	king can be provid sonation level is no ecurity for referenc	ded if authentication is used at anonymous. e tracking
	ОК	Cancel Apply

5. Go to the 'COM Security' tab. Under 'Access Permissions', click on the 'Edit Limits' button.

Ay Computer Prope	rties	? [
General	Options	Default Properties
Default Protocols	MSDTC	COM Security
Access Permissions You may edit who also set limits on a	is allowed default accomplications that determ	ess to applications. You may ine their own permissions.
Launch and Activativ You may edit who activate objects. Y determine their ow	on Permissions is allowed by default to 'ou may also set limits o n permissions. Edit Ljmits	p launch applications or on applications that Edit <u>D</u> efault
	ОК	Cancel Apply

6. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Access Permission		? 🔀
Security Limits		
<u>G</u> roup or user names:		
ANONYMOUS LOGO	N	
S NETWORK		
🕵 SYSTEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for SYSTEM	Allow	Deny
Local Access		
Remote Access	 	
1		
	(OK)	Cancel

7. Under 'Access Permissions', select the 'Edit Default' button.

My Computer Propert	ies	? 🛛
General Default Protocole	Options MSDTC	Default Properties
Access Permissions You may edit who is also set limits on app	allowed default access plications that determine	to applications. You may their own permissions.
	E dit <u>L</u> imits	Edit Default
Launch and Activation You may edit who is activate objects. Yo determine their own	n Permissions : allowed by default to lat u may also set limits on a permissions.	unch applications or applications that
	Edit Limits	Edit <u>D</u> efault
	ОК	Cancel Apply

8. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Access Permission		? 🗙
Default Security		
Group or user names:		
ANUNYMOUS LUGUN Everyone INTERACTIVE NETWORK SYSTEM		
Permissions for ANONYMOUS	Add	<u>R</u> emove Deny
Local Access Remote Access	Y Y	
	C. OK] Cancel

9. Under 'Launch and Activation Permissions', select 'Edit Limits'.

My Computer Properties	? 🛛
General Options Default Protocols MSDTC	Default Properties COM Security
Access Permissions You may edit who is allowed default acces also set limits on applications that determin	is to applications. You may e their own permissions.
Edit <u>L</u> imits	Edit Default
Launch and Activation Permissions You may edit who is allowed by default to I activate objects. You may also set limits on determine their own permissions.	aunch applications or applications that Edit <u>D</u> efault
ОК	Cancel <u>A</u> pply

10. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Launch Permission	? 🛛
Security Limits	
<u>G</u> roup or user names:	
🕵 ANONYMOUS LOGON	
Everyone INTERACTIVE NETWORK	
SYSTEM	
	A <u>d</u> d <u>R</u> emove
Permissions for ANUNYMOUS	Allow Deny
Local Launch	
Remote Launch	
Remote Activation	
	OK Cancel

My Computer Propert	ies	? 🛛
General Default Protocols	Options MSDTC	Default Properties COM Security
Access Permissions You may edit who is also set limits on ap	allowed default access t plications that determine t	o applications. You may heir own permissions.
	Edit <u>L</u> imits	<u>E</u> dit Default
Launch and Activation You may edit who is activate objects. Yo determine their own	n Permissions s allowed by default to lau umay also set limits on a permissions.	nch applications or pplications that
	Edit Limits	Edit <u>D</u> efault
	ОК С	Cancel <u>Apply</u>

11. Under 'Launch and Activation Permissions' select 'Edit Default'.

12. Ensure that you have allowed permissions to 'Anonymous Logon', 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Launch Permission	? 🛛
Default Security	
Group or user names:	
🐼 ANONYMOUS LOGON	
Everyone INTERACTIVE NETWORK SYSTEM	
Permissions for ANONYMOUS	Add <u>R</u> emove
Local Launch	
Remote Launch	
Local Activation Remote Activation	
	OK Cancel

13. We have successfully configured the default DCOM settings. Click OK to return to the Component Services window.

Default Protocols MSDTC COM Security Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions. Edit Limits Edit Default Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Edit Limits Edit Default	MSDTC	COM Security
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions. Edit Limits Edit Default Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Edit Limits Edit Limits Edit Default		
You may edit who is allowed default access to applications. You mails also set limits on applications that determine their own permissions. Edit Limits Edit Default		
Edit Limits Edit Default Launch and Activation Permissions	allowed default access ications that determine	s to applications. You m e their own permissions.
aunch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Edit Limits Edit <u>D</u> efault	Edit <u>L</u> imits	<u>E</u> dit Default
	allowed by default to la may also set limits on ermissions. Edit Limits	aunch applications or applications that Edit Default
	E dit Ejinito	
		allowed default access cations that determine Edit Limits Permissions allowed by default to la may also set limits on ermissions. Edit Limits

14. Under 'My Computer', open the folder labelled 'DCOM Config'

🖗 Component Services						X
🐌 Eile Action Yiew <u>W</u> indow Help					_6	١×
⇔ → 🗈 📧 🗙 💣 🔮 😫 '	Ê <u>∎</u> •	🗄 🗰 🗰 🗄	1			
Console Root	DCOM Config					
Component Services	((^
My Computer OM+ Applications DCOM Config	%Ip6FwHlp	AccStore Class	AcroPDF	ADM Document	Adobe Acrobat 7	
🕀 🦘 %Ip6FwHlpDispla 🕀 🥎 AccStore Class			P			
AcroPDF ADM Document	Automatic Updates	Background Intelligen	BarControl	Blocked Drivers	BrowserColl	
H State Acrobat 7. H State Automatic Update B Sackground Intelli						
BarControl Societation	CdlsHand	CodeBaby Object	COM+ Event System	ComEvents. ComService	ComEvents. ComSystem	
⊕						
CodeBabyObject COM+ Event Syst	Command line Trigger Co	CryptoSupport	CustReg Class	dfuicom	Diskeeper FAT engine	
ComEvents.com5 ComEvents.com5 ComEvents.com5 Command line Tric						
	Diskeener GUI	Diskeener	Diskeener	DPCnrniect	dne ocr	~

15. Browse to your OPC Server, right-click on it, and select 'Properties'.



16. Under the 'General' tab, set the Authentication Level to 'Connect'.

M	atrikon OP(C Server f	for Simulation and Testing Prop ?	×	
٢	General Loc	ation Secu	urity Endpoints Identity		
	General properties of this DCOM application				
	Applicatio	on Name:	Matrikon OPC Server for Simulation and Testing		
	Applicatio	on ID:	{F8582CF3-88FB-11D0-B850-00C0F0104305}		
	Applicatio	on Type:	Local Service		
	Authentic	ation Level:	Connect		
	Service Name: Matrikon OPC Server for Simulation and Testing				
			OK Cancel Apply		

17. Go to the 'Security' tab. Under 'Launch and Activation Permissions', select the 'Customize' button. Then click Edit.

Matrikon OPC Server for Simulation and Test	ing Prop ? 🔀
General Location Security Endpoints Identity	
Launch and Activation Permissions	[
Access Permissions	[<u>Edit]</u>
 Use Default Customize 	Edit
Configuration Permissions	
⊂ Use Defa <u>u</u> lt	
	E djt
OK Cano	el <u>Apply</u>

18. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Launch Permission		? 🛛
Security		
<u>G</u> roup or user names:		
Everyone Everyone Everyone Everyone Everyone Everyone Everyone Everyone		
SYSTEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for SYSTEM	Allow	Deny
Local Launch Remote Launch Local Activation Remote Activation		
	0K] Cancel

19. Under 'Access Permissions' choose the 'Customize' button. Then click Edit.

Matrikon OPC Serve	r for Simula	tion and '	Testing Prop	? 🛛
General Location	ecurity Endpo	oints Identit	y	
Launch and Activ	ation Permissio	ns		
C <u>U</u> se Default				
Customize			<u>E</u> dit	
Access Permissio	ns			
🔿 Use De <u>f</u> ault				
Customize			E <u>d</u> it)
Configuration Per	missions			
C Use Defa <u>u</u> lt				
Customize			Edįt	
		K) [Cancel	Apply

20. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Ac	cess Permission		? 🗙
S	ecurity		
	<u>G</u> roup or user names:		
	Everyone INTERACTIVE NETWORK		
	🕵 SYSTEM		
		A <u>d</u> d	<u>R</u> emove
	Permissions for SYSTEM	Allow	Deny
	Local Access Remote Access	▼	
		OK	Cancel

21. Go to the 'Identity' tab. Ensure that your server is either running as 'The interactive user' OR, if it is running as a service, 'The system account'. Click OK to return to the Component Services window.

General	Location	Security	Endpoints	Identity	
Which	user accour	nt do you v	want to use ti	o run this applic	ation?
G Th					
© The	interactive	user.			
⊖ The	Jaunching	user.			
C Thi	s <u>u</u> ser.	г			1
Us <u>e</u> r:					Browse
Pass	word:	ſ			
Co <u>n</u> fi	m passwor	d: 🛛			
O The	: system ac	count (serv	vices only).		
		(OK	Cance	

22. In the 'DCOM Config' folder browse to 'OpcEnum'. Right click on it and select 'Properties'.

Scomponent Services	
🚱 File Action View Window Help	_8_×
← → € 📧 × 🖀 🖉 😫 🏷 ┺ 🗄 🖷 🖷 📟	
Microsoft.Aspnet.Snapin.AspNetManagementUtilit: Microsoft.Aspnet.Snapin.AspNetManagementUtilit.AspNetMan	(\$)
Opens property sheet for the current selection.	

23. Under the 'General' tab ensure that the Authentication Level is set to 'Connect'.

OpcEnum Properties	? 🔀
General Location Secu	urity Endpoints Identity
General properties of th	is DCOM application
Application Name:	OpcEnum
Application ID:	{13486D44-4821-11D2-A494-3CB306C10000}
Application Type:	Local Service
Authentication Level:	Connect
Service Name:	OpcEnum
<u> </u>	

24. Go to the 'Security' tab. Under 'Launch and Activation Permissions', select the 'Customize' button. Then click Edit.

OpcEnum Properties	? 🔀
General Location Security Endpoints Identity	
Launch and Activation Permissions	
C Use Default	
Customize	<u></u> dit
Access Permissions	
C Use De <u>f</u> ault	
Customize	E <u>d</u> it
Configuration Permissions	
⊂ Use Defa <u>u</u> lt	
Customize	Edįt
OK Cano	el <u>A</u> pply

25. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Launch Permission		? 🔀
Security		
<u>G</u> roup or user names:		
🕵 Everyone		
1 INTERACTIVE		
TT STOLEM		
	A <u>d</u> d	<u>H</u> emove
Permissions for Everyone	Allow	Deny
Local Launch		
Remote Launch		
Remote Activation		

26. Under 'Access Permissions' select the 'Customize' button. Then click Edit.

OpcEnum Properties
General Location Security Endpoints Identity
Launch and Activation Permissions
C Use Default
Customize <u>E</u> dit
Access Permissions
C Use De <u>f</u> ault
Customize
Configuration Permissions
C Use Default
Customize Edit
OK Cancel Apply

27. Ensure that you have allowed permissions to 'Everyone', 'Interactive', 'Network', and 'System' as shown below. Then click OK.

Access Permission		? 🛛
Security		
Group or user names:		
Everyone INTERACTIVE METWORK SYSTEM		
	A <u>d</u> d	<u>R</u> emove
Permissions for SYSTEM	Allow	Deny
Local Access Remote Access	>	
	OK.] Cancel

28. Go to the 'Identity' tab. The user should be set to 'The system account', as OpcEnum runs as a service. Click OK. The DCOM settings on this machine are now correct.

OpcEnum Properties	? 🛛
General Location Security	y Endpoints Identity
Which user account do you	want to use to run this application?
C. The interactive user	
C The Jaunching user.	
⊂ This <u>u</u> ser.	
Us <u>e</u> r:	Browse
<u>P</u> assword:	
Confirm password:	
The system account (se	rvices only).
	OK Cancel Apply

The Windows Firewall

If the Windows Firewall is up and running, it will interfere with communication between applications on the system. There are ways to specify which applications are allowed through the Firewall – if you wish to do so, documents are available from the OPC Foundation which describe the procedure (www.opcfoundation.org). Otherwise disable the firewall by walking through the following steps:

1. Go to 'Start->Control Panel' as shown:



2. Double click on the 'Windows Firewall' icon.



3. Set the Windows Firewall to 'Off' as shown, and click OK. The Firewall will no longer block OPC Communication.



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 Service Pack 2 (SP2) and Microsoft Windows XP Tablet PC Edition 2005, DEP is enforced by hardware and by software.

DEP will also prevent many installations from running, and has been known to cause other software issues. Please disable it as per the following steps:

1. From your Start menu, right-click on 'My Computer' and select

'Properties'



2. Go to the 'Advanced' tab. Under 'Performance', hit the Settings button.

tem Properti	es			?
System Rest	ore	Automa	itic Updates	Remote
General	Comput	er Name	Hardware	Advanced
You must be log Performance Visual effects,	ged on as a processor s	an Administra cheduling, m	tor to make mos emory usage, ar	t of these changes. nd virtual memory
				<u>S</u> ettings
User Profiles				
Desktop setting	gs related to	o your logon		
				S <u>e</u> ttings
Startup and Re	covery			
System startup	, system fail	lure, and deb	ugging informati	on
				Settings
	Env	iro <u>n</u> ment Vari	ables E	rror Reporting

3. Select the 'Turn on DEP for essential....' button, as shown. Click OK. At this point it may be necessary to restart the machine.

Performance Options	? 🗙
Visual Effects Advanced Data Execution Prevention	
 Data Execution Prevention (DEP) helps protect against damage from viruses and other security threats. <u>How does it work?</u> <u>Turn on DEP for essential Windows programs and services only</u> <u>Turn on DEP for all programs and services except those I select:</u> 	
Add Remove Your computer's processor does not support hardware-based DEP. However, Windows can use DEP software to help prevent some types of attacks.	t

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 that these changes may compromise the security of your system – speak with your network administrator if you have any concerns.

1. Go to 'Start->Settings->Control Panel->Administrative Tools->Local Security Policy'.



- Go to 'Security Settings->Local Policies->Security Options'.
 Right-click on 'DCOM: Machine Access Restrictions...' and select 'Properties'.

ile Action View Help			
	ิด		
Security Settings	Policy A	Security Setting	
	Accounts: Administrator account status	Enabled	
🖶 🛄 Local Policies	Accounts: Guest account status	Disabled	
Augur Policy	Accounts: Limit local account use of b	Enabled	
Security Ontions	Accounts: Rename administrator acc	Administrator	
Public Key Policies	Accounts: Rename guest account	Guest	
Software Restriction Policie	Audit: Audit the access of global syst	Disabled	
🖳 IP Security Policies on Loca	Audit: Audit the use of Backup and R	Disabled	
-	Audit: Shut down system immediately	Disabled	
	BDCOM: Machine Access Restrictions i	O:BAG:BAD:(A::CCDCLC:::WD)(A;;CCDC;;;AN)	
	DCOM: Machine Launch Restrictions i	Not definit in operates	
	Devices: Allow undock without having	Enabled Help	
	Devices: Allowed to format and eject	Administrators	
	Devices: Prevent users from installing	Disabled	
	Devices: Restrict CD-ROM access to I	Disabled	
	Devices: Restrict Hoppy access to loc	Disabled	
	Devices: Unsigned driver installation	Silently succeed	
	Domain controller: Allow server opera	Not defined	
	Domain controller: LDAP server signin	Not derined	
	Domain controller: Refuse machine ac	Not defined	
	Domain member: Digitally encrypt or	Enabled	
	Domain member: Digitally encrypt sec	Enabled	
	Domain member: Digitally sign secure	Enabled Disabled	
	Domain member: Disable machine acc	Disabled	
	Domain member: Maximum machine a	ou days	
	Domain member: Require strong (win	Disabled	
	The interactive logon: Do not usplay last	Disableu Net defined	
	Theractive logon: Do not require CT	Not defined	
	Theractive logon: Message text for u	Not defined	
	Theractive logon: Number of previou	10 logops	
	Interactive logon: Number of previou	5 days	
	State active logon: Pequire Domain Co	Dicabled	
	Differentive logon: Require smart card	Not defined	
	bo Interactive logon: Smart card remova	No Action	
	Microsoft network client: Digitally sign	Disabled	
	Microsoft petwork clienty Digitally sign	Enabled	

4. Hit the 'Edit Security' button, as shown.

DCOM: Machine Access Restrictions in Security Descri 🕐 🔀
Template Security Policy Setting
DCOM: Machine Access Restrictions in Security Descriptor Definition Language (SDDL) syntax
If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.
Security descriptor:
0:BAG:BAD:(A;;CCDCLC;;;WD)(A;;CCDC;;;AN)
OK Cancel Apply

5. Ensure that 'Everyone', 'Interactive', 'Network', and 'System' are added into the allowed Group or User Names, as shown. Click OK to return to the main security policy window.

<u>G</u> roup or user names:		
🕵 Everyone		
1 INTERACTIVE		
SYSTEM		
	A <u>d</u> d	<u>R</u> emov
Permissions for SYSTEM	Allow	Deny
Local Access	~	
Remote Access	\checkmark	

6. Right-click on 'DCOM: Machine Launch Restrictions...' and select 'Properties'.

File Action View Holo			
	ฉ		
	5	[]	
	Policy A	Security Setting	
	Accounts: Administrator account status	Enabled	
	Accounts: Guest account status	Disabled	
🗄 词 User Rights Assignmen	Accounts: Limit local account use of b	Enabled	
Gecurity Options	Accounts: Rename administrator acc	Administrator	
Public Key Policies	Accounts: Rename guest account	Guest	
🖂 🚞 Software Restriction Policie	Audit: Audit the use of Padus and D	Disabled	
🗄 🜏 IP Security Policies on Loca	Audit: Audit the use of Backup and R	Disabled	
	BOCOM Machina Assass Pactrictions i		
	DCOM: Machine Launch Restrictions i	Not defined	
	Devices: Allow underk without having	Footbed Properties	
	Big Devices: Allowed to format and eject	Administrators Help	
	Bill Devices: Prevent users from installing	Dicabled	
	Bo Devices: Restrict CD-ROM access to I	Disabled	
	Devices: Restrict floppy access to loc	Disabled	
	Devices: Unsigned driver installation	Silently succeed	
	Domain controller: Allow server opera	Not defined	
	Domain controller: LDAP server signin	Not defined	
	Domain controller: Refuse machine ac	Not defined	
	Domain member: Digitally encrypt or	Enabled	
	Domain member: Digitally encrypt sec	Enabled	
	Domain member: Digitally sign secure	Enabled	
	Bomain member: Disable machine acc	Disabled	
	Bomain member: Maximum machine a	30 days	
	Bomain member: Require strong (Win	Disabled	
	👪 Interactive logon: Do not display last	Disabled	
	Interactive logon: Do not require CT	Not defined	
	👪 Interactive logon: Message text for u		
	👪 Interactive logon: Message title for u	Not defined	
	BIInteractive logon: Number of previou	10 logons	
	🚰 Interactive logon: Prompt user to cha	5 days	
	👪 Interactive logon: Require Domain Co	Disabled	
	👸 Interactive logon: Require smart card	Not defined	
	🔀 Interactive logon: Smart card remova	No Action	
	🗮 Microsoft network client: Digitally sign	Disabled	
	🔀 Microsoft network client: Digitally sign	Enabled	

7. Hit the 'Edit Security' button, as shown.

DCOM: Machine Launch Restrictions in Security Descr 🕐 🔀
Template Security Policy Setting
DCOM: Machine Launch Restrictions in Security Descriptor Definition Language (SDDL) syntax
If the security descriptor is left blank after defining the policy setting in the template, the policy setting will not be enforced.
Security descriptor:
OK Cancel Apply

8. Ensure that 'Everyone', 'Interactive', 'Network', and 'System' are added into the allowed Group or User Names, as shown. Click OK to return to the main security policy window.

ita- 1 ia-ita-	
<u>G</u> roup or user names:	
🕵 Everyone	
🕵 INTERACTIVE	
🕵 NETWORK	
SYSTEM	
	Add <u>R</u> emov
Permissions for SYSTEM	Allow Deny
Local Launch	
Remote Launch	
Local Activation	
Remote Activation	

9. Browse to 'Network access: Let Everyone permissions apply to anonymous users'. Right click on it, and select 'Properties'.

File Action View Help					
- → 🗈 🗙 🗗 😼 🖆	8				
Security Settings	Policy 🛆	Security Setting			
- 📴 Account Policies	Interactive logon: Message title for users attempting to log on	Not defined			
📴 Local Policies	Interactive logon: Number of previous logons to cache (in case domain c	10 logons			
🖅 🧾 Audit Policy	Interactive logon: Prompt user to change password before expiration	5 days			
🕀 🧾 User Rights Assignmen	BInteractive logon: Require Domain Controller authentication to unlock wo	Disabled			
Security Options	Interactive logon: Require smart card	Not defined			
Public Key Policies	BInteractive logon: Smart card removal behavior	No Action			
TD Security Delicies on Loss	Microsoft network client: Digitally sign communications (always)	Disabled			
- Security Policies of Loca	Microsoft network client: Digitally sign communications (if server agrees)	Enabled			
	BMicrosoft network client: Send unencrypted password to third-party SMB	Disabled			
	Microsoft network server: Amount of idle time required before suspendin	15 minutes			
	Microsoft network server: Digitally sign communications (always)	Disabled			
	Microsoft network server: Digitally sign communications (if client agrees)	Disabled			
	Microsoft network server: Disconnect clients when logon hours expire	Enabled			
	Network access: Allow anonymous SID/Name translation	Disabled			
	Network access: Do not allow anonymous enumeration of SAM accounts	Enabled			
	Wetwork access: Do not allow anonymous enumeration of SAM accounts	Disabled			
	Network access: Do not allow storage of credentials or .NET Passports f	Disabled			
	Network access: Let Everyone permissions apply to anonymous users	Enabled		-	
	BNetwork access: Named Pipes that can be accessed anonymously	COMNAP, COMNODE, SQL\QL	Properties	C,browser	
	BNetwork access: Remotely accessible registry paths	System\CurrentControlSet\C	Help	s,System\Curr	
	BNetwork access: Shares that can be accessed anonymously	COMCFG,DFS\$. ioip	1	
	BNetwork access: Sharing and security model for local accounts	Classic - local users authentical	te as themselves		
	👸 Network security: Do not store LAN Manager hash value on next passwo	Disabled			
	BNetwork security: Force logoff when logon hours expire	Disabled			
	BNetwork security: LAN Manager authentication level	Send LM & NTLM responses			
	BNetwork security: LDAP client signing requirements	Negotiate signing			
	BNetwork security: Minimum session security for NTLM SSP based (includin	No minimum			
	BNetwork security: Minimum session security for NTLM SSP based (includin	No minimum			
	BRecovery console: Allow automatic administrative logon	Disabled			
	BRecovery console: Allow floppy copy and access to all drives and all folders	Disabled			
	🔀 Shutdown: Allow system to be shut down without having to log on	Enabled			
	🞉 Shutdown: Clear virtual memory pagefile	Disabled			
	By System cryptography: Use FIPS compliant algorithms for encryption, has	Disabled			
	Bystem objects: Default owner for objects created by members of the A	Object creator			
	👸 System objects: Require case insensitivity for non-Windows subsystems	Enabled			
	System objects: Strengthen default permissions of internal system objec	Enabled			

10. Select 'Enabled' and click 'OK'.

Network access: Let Everyone permissions apply to a 🕐 🔀
Local Security Setting
Network access: Let Everyone permissions apply to anonymous users
● Enabled
O Di <u>s</u> abled
OK Cancel Apply

11. Browse to 'Network access: Sharing and security model for local accounts'. Right-click on it and select 'Properties'.

Local Security Settings			_ 0
File Action View Help			
← → 🗈 X 🗗 😼 🕯	3		
Security Settings	Policy A	Security Setting	
E 📴 Account Policies	Interactive logon: Message title for users attempting to log on	Not defined	
Local Policies	Interactive logon: Number of previous logons to cache (in case domain c	10 logons	
Audit Policy	PInteractive logon: Prompt user to change password before expiration	5 days	
User Rights Assignmen	Interactive logon: Require Domain Controller authentication to unlock wo	Disabled	
Bublic Key Policies	🕮 Interactive logon: Require smart card	Not defined	
Software Destriction Policie	🕮 Interactive logon: Smart card removal behavior	No Action	
IP Security Policies on Loca	Bi Microsoft network client: Digitally sign communications (always)	Disabled	
📺 μη declarky romoles of Loca	Microsoft network client: Digitally sign communications (if server agrees)	Enabled	
	Microsoft network client: Send unencrypted password to third-party SMB	Disabled	
	Microsoft network server: Amount of idle time required before suspendin	15 minutes	
	BigMicrosoft network server: Digitally sign communications (always)	Disabled	
	Bill Microsoft network server: Digitally sign communications (if client agrees)	Disabled	
	Microsoft network server: Disconnect clients when logon hours expire	Enabled	
	WNetwork access: Allow anonymous SID/Name translation	Disabled	
	Wetwork access: Do not allow anonymous enumeration of SAM accounts	Enabled	
	Wetwork access: Do not allow anonymous enumeration of SAM accounts	Disabled	
	Wetwork access: Do not allow storage of credentials or .NET Passports f	Disabled	
	Network access: Let Everyone permissions apply to anonymous users	Enabled	
	Network access: Named Pipes that can be accessed anonymously	COMNAP,COMNODE,SQL\QUERY,SPOOLSS,LLSRPC,browser	
	Network access: Remotely accessible registry paths	System\CurrentControlSet\Control\ProductOptions,System\Curr	
	Network access: Shares that can be accessed anonymously	COMCFG,DF5\$	
	Network access: Sharing and security model for local accounts	Classic - local users authenticate as themselves	1
	Network security: Do not store LAN Manager hash value on next passwo	Disabled	
	Network security: Force logoff when logon hours expire	Disabled Help	
/	Network security: LAN Manager authentication level	Send LM & NTLM responses	
	Network security: LDAP client signing requirements	Negotiate signing	
	Network security: Minimum session security for NTLM SSP based (includin	No minimum	
	Network security: Minimum session security for NTLM SSP based (includin	No minimum	
	Recovery console: Allow automatic administrative logon	Disabled	
	Recovery console: Allow floppy copy and access to all drives and all folders	Disabled	
	Shutdown: Allow system to be shut down without having to log on	Enabled	
	Shutdown: Clear virtual memory pagefile	Disabled	
	5ystem cryptography: Use FIPS compliant algorithms for encryption, has	Disabled	
	5ystem objects: Default owner for objects created by members of the A	Object creator	
	5ystem objects: Require case insensitivity for non-Windows subsystems	Enabled	
	System objects: Strengthen default permissions of internal system objects	Epabled	

12. Select 'Classic – local users authenticate as themselves' and click OK.

Network access: Sharing and security model for local ? 🔀		
Local Security Setting		
Network access: Sharing and security model for local accounts		
Classic - local users authenticate as themselves		
OK Cancel Apply		

Your **<u>DCOM</u>** is now setup to accept all incoming connections.

<u>NOTE</u>: DCOM has limitations for connectivity when operating on separate domains/workgroups. These steps may work but, depending on individual networks, additional settings and components may be required. Please contact OPC Support for additional information.

Phone:	+1-780-945-4011
E-Mail:	Support@MatrikonOPC.com
Web:	www.OPCSupport.com