



Member of: KNX Association | OPC Foundation BACnet Interest Group Europe

BACnet"

BODC°

KNX

Document Version: 1.0.2

NETX AUTOMATION

Contents

1.	General	4
2.	Windows Firewall Configuration 2.1. Allow DCOM communication from other computers 2.2. Creating a rule for OPC enum 2.3. Creating a rule for the NETx Server 2.4. Creating a rule for the OPC client	5 6 7 8
3.	Changing the local security policy	9
4.	User settings 4.1. Both machines are member of the same Windows domain	10 10 10 11
5.	DCOM configuration 5.1. DCOM configuration at the NETx Server side 5.1.1. Configure default DCOM settings 5.1.2. Configure DCOM settings of OPC enum 5.1.3. Configure DCOM settings of NETx Server 5.2. DCOM configuration at the OPC client side	12 12 14 15 15
Α.	Appendix A.1. Support and contact	16 16



Copyright

This published handbook refers to the release of NETx DCOM Setting Documentation 1.0. The software is published by NETxAutomation Software GmbH, Maria–Theresia–Straße 41, Top 10, 4600 Wels, Austria.

© Copyright by NETxAutomation Software GmbH, 2014. The correct and usable documentation can only be guaranteed in connection with the regulations of the software agreement. Changes regarding the size of the function volume of the mentioned software can be done and may not involve a change of the documentation.

All rights are reserved. Copies, translations, micro filming and the storage and processing in data processing systems are copyrighted. No part of this publication may be reproduced without the prior permission of the publisher NETxAutomation Software GmbH.



1. General

In order to enable an OPC DA 2.05a communication between an OPC server and one or more OPC clients, different configuration steps are necessary. This includes a change of the Windows Firewall settings as well as the configuration of the Windows DCOM system and its security policy. This documentation shall act as a tutorial for configuring a remote OPC DA 2.05a connection.

! Configuring Windows DCOM can be complex and time consuming. In addition, OPC DA communication may not be possible at all if, for example, the OPC server and the OPC clients are not in the same LAN. Therefore, NETxAutomation Software GmbH provides a solution called NETx Tunneller. The NETx Tunneller is a software tool that tunnels the OPC communication through a VNET connection. VNET is a proprietary protocol provided by NETxAutomation Software GmbH. VNET is based on a TCP/IP connection and thus a time consuming Windows DCOM configuration is not necessary. More information about the NETx Tunneller can be found at the website of NETxAutomation Software GmbH (www.netxautomation.com).

This documentation shows the necessary configuration steps for setting up such a remote OPC DA 2.05a connection. Within this documentation, it is assumed that OPC server is either a NETx BMS Server or a NETx KNX OPC Server. For the rest of this documentation, the OPC server is simply referred to as NETx Server.

The remote OPC client that shall connect to the NETx Server can be an OPC DA 2.05a client from any vendor. For the rest of this documentation, a remote OPC DA 2.05a client is simply referred to as OPC client.

! As OPC client, clients that support OPC DA 3.0 can be used too since these clients are backward compatible to OPC DA 2.05a.

In addition, it is assumed that the NETx Server and the OPC client are running under one of the following operating systems:

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2

Note that other Windows versions may work too. However, it is not guaranteed that the configuration steps described within this document are sufficient for unsupported operating systems.

!Attention: Please keep in mind that this documentation shall only act as an example how an OPC connection can be established. It is not guaranteed that this documentation is complete and that the described configuration steps fulfil the safety and security requirements of the IT infrastructure where it is applied. Changes to configuration settings could result in insufficient safety and security. Therefore, any change has to be reviewed and approved by the local system/security administrator.

In order to enable an OPC communication between an OPC server and one or more OPC clients, the following steps are necessary:

- Configuring the Windows Firewall (cf. chapter 2).
- Changing the local security policy (cf. chapter 3).
- Setting up a user (cf. chapter 4).
- Configuring Windows DCOM (cf. chapter 5).



2. Windows Firewall Configuration

In order to permit OPC communication, the Windows Firewall has to be configured accordingly. This section described the necessary steps that have to be performed.

2.1. Allow DCOM communication from other computers

Attention: These steps have to be performed at both sides – at the OPC server and at the OPC client side.

By default, Windows blocks inbound DCOM connections from other computers. Therefore, the following steps have to be performed:

Open the Windows Firewall configuration dialogue (Control panel -> System and Security -> Windows Firewall) and select "Advanced settings" at the left hand side of the dialogue. The following dialogue appears (cf. figure 2.1).



Figure 2.1.: Windows Firewall configuration

Select "Inbound Rules" and enable the all rules that are named "Windows Management Instrumentation (DCOM-In)" (cf. figure 2.2).

<i>₽</i>	Windows Firewall with Ad	vanced Security			- 0	>
File Action View Help						
🗧 🔿 🙍 📷 🚱 🖬 📷						
Windows Firewall with Advan	Inbound Rules				Actions	
Cuthound Rules	Name	Group	Profile	Enat ^	Inbound Rules	
Connection Security Rules	TPM Virtual Smart Card Management (TCP-In)	TPM Virtual Smart Card Ma	Domain	No	Kew Rule	
Nonitoring	TPM Virtual Smart Card Management (TCP-In)	TPM Virtual Smart Card Ma	Private,	No	Filter by Profile	
	Wirtual Machine Monitoring (DCOM-In)	Virtual Machine Monitoring	All	No	The of the	
	Wirtual Machine Monitoring (Echo Request - ICMPv4-In)	Virtual Machine Monitoring	All	No	Y Filter by State	
	Wirtual Machine Monitoring (Echo Request - ICMPv6-In)	Virtual Machine Monitoring	All	No	Filter by Group	
	Wirtual Machine Monitoring (NB-Session-In)	Virtual Machine Monitoring	All	No	View	
	Wirtual Machine Monitoring (RPC)	Virtual Machine Monitoring	All	No	Defust	
	🕼 Wi-Fi Direct Network Discovery (In)	Wi-Fi Direct Network Discov	Public	Yes	Ca Neresti	
	Wi-Fi Direct Scan Service Use (In)	Wi-Fi Direct Network Discov	Public	Yes	Export List	
	Wi-Fi Direct Spooler Use (In)	Wi-Fi Direct Network Discov	Public	Yes	Help	
	Windows Collaboration Computer Name Registration Servic	Windows Collaboration Co	All	No	-	
	Windows Collaboration Computer Name Registration Servic	Windows Collaboration Co	All	No	Windows Manageme.	
	Windows Firewall Remote Management (RPC)	Windows Firewall Remote	Domain	No	Disable Rule	
	Windows Firewall Remote Management (RPC)	Windows Firewall Remote	Private,	No	X Cut	
	Windows Firewall Remote Management (RPC-EPMAP)	Windows Firewall Remote	Domain	No		
	Windows Firewall Remote Management (RPC-EPMAP)	Windows Firewall Remote	Private,	No	Copy	
	Windows Management Instrumentation (ASync-In)	Windows Management Instr	Private,	No	🗙 Delete	
	Minutows Management Instrumentation (Asymetra)	Windows Management Instr	Domain	No	Properties	
	Windows Management Instrumentation (DCOM-In)	Windows Management Instr	Private,	Yes	17 Male	
	Windows Management Instrumentation (DCOM-In)	Windows Management Instr	Domain	Yes	In theip	
	Windows Management Instrumentation (VA # 49)	Windows Management Instr	Domain	No		
	Windows Management Instrumentation (W/M-In)	Windows Management Instr	Drivate	No		

Figure 2.2.: Enable "Windows Management Instrumentation (DCOM-In)"

! Depending on the operating system and on the used configuration, one or more DCOM-In rules can exist. If on rules exist, create two inbound rules to allow TCP port 135 and UDP port 135.



2.2. Creating a rule for OPC enum

```
Attention: These steps have to be performed at the OPC server side only.
```

An inbound rule for the OPC Enum process has to be added. On the top left corner, select "Inbound rules ...". Afterwards, click "New Rule ..." at the top right corner. Within the dialog, select "Program" as rule type (cf. figure 2.3).

@	New Inbound Rule Wizard
Rule Type Select the type of firewall ru	e to create.
Steps:	What have of a fer you do you like to proste?
 Hule lype Program Action Profile Name 	Program Fuel that controls connections for a program. O Port Rule that controls connections for a TCP or UDP port.
	Predefined: BranchCache - Cortext Retrieval (Uses HTTP) V Rule that controls connections for a Windows experience. Oustom Custom Custom

Figure 2.3.: New firewall rule

In the next step, select the executable file of the OPC enum process (cf. figure 2.4). It is located at:

• 32 bit operating sytem:

C:\Windows\System32\OpcEnum.exe

• 64 bit operating sytem:

C:\Windows\SysWOW64\OpcEnum.exe

<i>₽</i>	New Inbound Rule Wizard
Program Specify the full program path	and executable name of the program that this rule matches.
Steps: Pule Type Program	Does this rule apply to all programs or a specific program?
Action Profile Name	All programs Rule applies to all connections on the computer that match other rule properties. This program path:
	%SystemRoot %\SyeWOW64\OpcErum exe Browse Example: c/vath/upogram.exe %PogramFles%/browser/browser.exe

Figure 2.4.: Select program

Next, select "Allow the connection" (cf. figure 2.5).



Figure 2.5.: Allow the connection



As next step, select the network profile(s) for with the rule shall be active (cf. figure 2.6).

@	New Inbound Rule Wizard	×
Profile Specify the profiles for which	this rule applies.	
Steps:		
Rule Type	When does this rule apply?	
Program		
Action	✓ Domain	
Profile	Applies when a computer is connected to its corporate domain.	
Name	✓ Private	
	Applies when a computer is connected to a private network location, such as a home or work place.	
	✓ Public	
	Applies when a computer is connected to a public network location.	

Figure 2.6.: Select network profile

Finally, specify a name for rule (e.g. "OPC enum") (cf. figure 2.7).

@	New Inbound Rule Wizard	×
Name Specify the name and desc	ription of this rule.	
Steps:		
Rule Type		
Program		
Action		
Profile	Name:	
Name	OPC Enum	
	Description (optional):	

Figure 2.7.: Specify a rule name

After having confirmed the last step, a new rule is created and activated immediately.

2.3. Creating a rule for the NETx Server

Attention: These steps have to be performed at the OPC server side only.

It is required to permit communication to the NETx Server. The setup of the NETx Server is creating a corresponding firewall rule automatically. For the NETx BMS Server this rule is called "NETx BMS Server" – for the NETx KNX OPC Server it is called "NETx KNX OPC Server". If the corresponding rule is not listed, create a new one by performing the same steps as described within section 2.2. As program path (cf. figure 2.4), the executable of the NETx Server has to be specified. If the default installation directories are used, the executable of the NETx Server can be found here:

- NETx BMS Server:
 - 32 bit operating system:

C:\Program Files\NETxAutomation\NETx.BMS.Server.2.0

- 64 bit operating system:

C:\Program Files (x86)\NETxAutomation\NETx.BMS.Server.2.0

- NETx KNX OPC Server:
 - 32 bit operating system:

C:\Program Files\NETxAutomation\NETxKNX.OPC.3.5.UD

- 64 bit operating system:

C:\Program Files (x86)\NETxAutomation\NETxKNX.OPC.3.5.UD

! The rule that is automatically added by the setup is activated for the network profiles "Private" and "Domain" only. If the connected network is defined as "Public", the rules has to be changed accordingly.

NETx DCOM Setting Documentation 1.0.2



2.4. Creating a rule for the OPC client

Attention: These steps have to be performed at the OPC client side only.

It is also required to permit communication to the OPC client. Create a corresponding firewall rule by performing the same steps as in section 2.2. Within figure 2.4 select the OPC client executable.



3. Changing the local security policy

Attention: These steps have to be performed at both sides – at the OPC server and at the OPC client side.

In order to allow OPC communication, the local security policy has to be changed. Open the configuration dialogue ("Control panel -> System and Security -> Administrative Tools -> Local Security Policy") and navigate to "Security Settings -> Local Policies -> "Security Options" and enable the option "Network access: Let Everyone permissions apply to anonymous users" (cf. figure 3.1).

4	Local Security Policy		×
File Action View Help			
Security Settings Out Policies Cal Policie	Pelicy Microsoft network serve: Digitally sign communications (if client agrees) Microsoft network serve: Digitally sign communications (if client agrees) Microsoft network serve: Serve SPM ruge Thange name validation Microsoft network serve: Serve SPM ruge Thange name validation Microsoft network serves: Serve SPM ruge Thange name validation Microsoft network secress: Do not allow somerous enumeration of SMM accounts Microsoft network secress: Do not allow somerous enumeration of SMM accounts Microsoft network secress: Do not allow somerous enumeration of SMM accounts Microsoft network secress: Do not allow somerous enumeration of SMM accounts Microsoft accounts of Do not allow somerous dependentials for networks and Microsoft accounts Let Revenom partnersions aged by annonymous just Microsoft accounts Let Revenom partnersions aged by annonymous just Microsoft accounts Let Revenom be accessed annonymously	Security Setting Disabled Enabled Not Defined Disabled Disabled Disabled Enabled	>
 IP Security Policies on Local Compute Advanced Audit Policy Configuration 	Network access: Remotely accessible registry parts Network access: Remotely accessible registry paths and sub-paths	System\CurrentControlS System\CurrentControlS	

Figure 3.1.: Local security policy



4. User settings

To be able to establish an OPC connection between a NETx Server and an OPC client, the user management must be configured accordingly. In general, it is necessary that both PCs must have at least one common Windows user. This Windows user must use the same user name and password and it must have local administrator rights at both machines.

The NETx Server process does not need to run under the common user. It can be run under the user "SYSTEM" (default for NETx Servers) or any user that has administrator rights. However, the OPC client itself must run under the common user – otherwise the OPC communication will not work.

Depending on the used environment, the following configuration steps may be possible:

4.1. Both machines are member of the same Windows domain

Since both machines are member of the same Windows domain, they are using the same user database. This means any domain user can be used as common user. However, the common user must have local administrator rights at both machines. To add local administrator rights, open the Computer Management dialogue ("Control Panel –> System and Security –> Administrative Tools") and select "Computer Management –> System Tools –> Local Users and Groups –> Groups". Double click "Administrators" and add the common user to the local administrator group. Figure 4.1 shows the configuration dialogue.



Figure 4.1.: Add administrator rights

4.2. Both machines are member of different Windows domains

If both machines are member of different domains, trust must be established on both domain controllers. This means that the users of domain A must be trusted by domain B and vice versa. More information about setting up trusts between domains can be found in the Microsoft Windows Server documentation.

In addition, local administrator rights must be given to the common user at both machines. This can be done by using the same steps as shown in section 4.1 and figure 4.1.



4.3. Both machines are not member of a Windows domain

If both machines are not member of a Windows domain, a common user has to be created on both machines. This user must have exactly the same user name and the same password at both machines. In addition, the user must have administrator rights on both machines.



5. DCOM configuration

In order to enable OPC communication, the Windows DCOM configuration has to be adapted. This section describes the necessary steps that have to be performed.

To be able to change the DCOM configuration, the DCOM configuration manager has to be opened. It can be started by entering "dcomcnfg" within the Windows search function or by starting the executable file directly. The executable file can found here:

C:\Windows\System32\dcomcnfg.exe

5.1. DCOM configuration at the NETx Server side

The DCOM configuration at the NETx Server side consists of three steps:

- Configure default DCOM settings (cf. section 5.1.1)
- Configure DCOM settings of OPC enum (cf. section 5.1.2)
- Configure DCOM settings of NETx Server(cf. section 5.1.3)

5.1.1. Configure default DCOM settings

First, the general DCOM settings have to changed. Within the DCOM configuration dialogue, right click at "My Computer", select "Properties", and change to the tab "Default Properties". Within this tab, ensure that the "Authentication Level" is set to "None". Figure 5.1 shows the resulting dialogue.

General	Options	Default	Properties
Verault Distributed COM C	ommunication m	openies	
The Authentientien Louis	the second second	at the analyst	level.

Figure 5.1.: Default Authentication level

Then, the limits of the DCOM security settings have to be changed. Change to the tab "COM Security". Figure 5.2 shows the resulting dialogue.



Figure 5.2.: Edit limits



Within "Access Permissions", press the button "Edit limits" and change the permissions of "Everyone" and "ANONY-MOUS LOGON" according to figure 5.3.

Security Limits	ccss remnssion	_	Access Permission
Group or user names: Everyone Call APPLICATION Company Destructed COM Use ANONYMOUS LOG	PACKAGES sers (WG-Win&x64-Test\F ers (WG-Win&x64-Test\D ON	Performance L istributed COM	Group or user names: Second or user names: LL APPLICATION PACKAGES Control Conductor of Users (WG-Win&64-Test/Performance Distributed COM Users (WG-Win&64-Test/Distributed Of AMONYMONIS LOGON
_			
Permissions for Everyone	Add	Remove	Permissions for ANONYMOUS

Figure 5.3.: Access Permissions

Then, close the dialogue and press the button "Edit limits" within "Launch and Activation Permissions". Change the permissions of "Everyone" and "Administrators" according to figure 5.4.

cunty units			
aroup or user names:		Group or user names:	
St. Everyone		Sector Se	
ALL APPLICATION PACKAGES		ALL APPLICATION PACKAGES	
Administrators (WG-Win8x64-Test	Administrators)	Administrators (WG-Win8x64-Test	Administrators)
Reformance Log Users (WG-Win&	k64-Test\Performance L	Reformance Log Users (WG-Win8	x64-Test\Performance L
Representation of the sense of	64-Test \Distributed COM	Sistributed COM Users (WG-Win&	64-Test\Distributed CON
A	Add Remove		Add Remove
Permissions for Everyone	Add Remove	Permissions for Administrators	Add Remove
Permissions for Everyone	Add Remove	Permissions for Administrators	Add Remove
Permissions for Everyone Local Launch Remote Launch	Add Remove	Permissions for Administrators Local Launch Remote Launch	Add Remove
Permissions for Everyone Local Launch Local Activation	Add Remove	Permissions for Administrators Local Launch Remote Launch Local Activation	Add Remove
Permissions for Everyone Local Launch Remote Launch Local Activation Remote Activation	Remove Image: Deny Image: Deny<	Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Add Remove

Figure 5.4.: Launch and Activation Permissions

Afterwards, the changes have to be confirmed by pressing the "OK" button.



5.1.2. Configure DCOM settings of OPC enum

As next, the DCOM security settings of the OPC enum process have to changed. Within the DCOM configuration dialogue, open the tree "DCOM Config" and locate the entry "OPCEnum". Right click at the entry, select "Properties", and change to the tab "General". Within this tab, ensure that the "Authentication Level" is set to "None". Figure 5.5 shows the resulting dialogue.

		Орс	Enum Pro	operties	? ×
General	Location	Security	Endpoints	Identity	
Gene App App	ral propertie lication Nar lication ID:	es of this D ne: Op {13	COM applica cEnum 1486D44-482	tion 21-11D2-A494-30	CB306C10000}
Арр	lication Typ	e: Loo	cal Service		
Auth	nentication	Level: No	one)	~
Sen	vice Name:	Up	cEnum		

Figure 5.5.: Authentication level

Then, change to the tab "Security". Within the "Launch and Activation Permissions", select "Customize" and press the "Edit" button. Change the permissions of "Everyone" and "Administrators" according to figure 5.6.

curity			Security		
aroup or user names: Leveryone SYSTEM Administrators (WG:Win8x64	I-Test\Administrators)		Group or user names:		
INTERACTIVE	Add	Remove		Add	Remove
emissions for Everyone	Allow	Deny	Permissions for Administrators	Allow	Deny
Local Launch			Local Launch		
Remote Launch			Remote Launch	-	
Local Activation			Local Activation	-	
Remote Activation			Remote Activation		

Figure 5.6.: Launch and Activation Permissions



Close the dialogue again. Within the "Access Permissions", select "Customize" and press the "Edit" button. Change the permissions of "Everyone" according to figure 5.7(a). Afterwards, close the dialogue. Within the "Configuration Permissions", select "Customize" and press the "Edit" button. Change the permissions of "Administrators" according to figure 5.7(b).

ecunty			Group or user names:		
Group or user names:			ALL APPLICATION	I PACKAGES	
& Evervone			& CREATOR OWNE	R	
SELF			SYSTEM		
SYSTEM			Administrators (WG	-Win8x64-Test\Admir	nistrators)
			THE LEARS (W/L S-W/LO SVE		
			Users (WG-Winaxa	4-Test (Users)	1
			as Users (WG-Winaxe	Add	Remove
	Add F	Remove	Permissions for Administr	Add	Remove Jon Deny
Permissions for Everyone	Add F	Remove	Permissions for Administr Full Control	Add	Remove
⁹ ermissions for Everyone Local Access	Add	Remove Deny	Permissions for Administr Full Control Read	Add	Remove

(a) Access Permissions

(b) Configuration Permissions

Figure 5.7.: OPC enum permissions

The DCOM configuration of the OPC enum process is finished now and the dialogue can be closed again.

5.1.3. Configure DCOM settings of NETx Server

Normally, changing the DCOM configuration for a NETx Server is not necessary since the DCOM setting are automatically created during the installation process of the NETx Server. However, if the OPC connection between the OPC client and the NETx Server is not working, it is recommended to verify whether the DCOM settings are correct.

The required DCOM configuration for a NETx Server is identical to the settings of the OPC enum process. To verify them, open the tree "DCOM Config" within the DCOM settings dialogue and locate the entry for the NETx Server. Depending on the type of server, the entries are named as follow:

- NETx BMS Server: "nxaVoyagerServer20"
- NETx KNX OPC Server: "NETxOPC"

After the correct entry has been found, apply the same configuration steps as described in section 5.1.2.

5.2. DCOM configuration at the OPC client side

The DCOM configuration the OPC client side is easier than at the NETx Server side, since only the default DCOM settings have to be changed. The required default DCOM settings at the client side are identical to the settings at the NETx Server side. Therefore, open the DCOM configuration dialogue and apply the same settings as described in section 5.1.1.



A. Appendix

A.1. Support and contact

Please send all your support questions to:

support@NETxAutomation.com

If you have general questions regarding the product and service please send your email to:

office@NETxAutomation.com