Exele OPC Products and Hardening DCOM Changes (KB5004442)

Latest update: December 20, 2021

Contents

Summary

"OPC Classic" is the term for OPC technology that relies on DCOM.

Due to a vulnerability detailed in CVE-2021-26414, Microsoft released a security update in June 2021 which will change the level of DCOM security required between OPC Classic clients and remote OPC servers. Once implemented, this change will cause connection failures between many OPC clients and remote OPC servers.

The change is being rolled out in phases to allow users to test the impact on DCOM and OPC products. Once the security updates of June 8, 2021 are applied:

- A registry setting (RequireIntegrityActivationAuthenticationLevel) can be added on the OPC server machine to enforce the new DCOM security level. OPC clients can then be tested.
- Planned for early Q1 2022: The new DCOM security level is enabled by default but can be disabled via the RequireIntegrityActivationAuthenticationLevel registry key if necessary.
- Planned for Q2 2022: New DCOM security level enabled and cannot be disabled.

Details of managing this change are available in Microsoft KB5004442.

Windows DCOM Security change

The new DCOM security level required by OPC Classic clients is "Packet Integrity" which authenticates and verifies that the transferred data has not been modified.

In order to use this new DCOM security level, it must be implemented in the client application. If the client application does not currently support Packet Integrity Authentication Level, updates from the OPC client vendor must be obtained to support Packet Integrity.

Which OPC clients will not be affected by this change?

The following OPC classic clients/servers are not affected by this change:

- OPC clients and servers on the same machine
- OPC clients that implement Packet Integrity authentication level
- Remote OPC clients and servers that use an OPC tunneller if the tunneller makes local OPC connections on both machines

How does this issue present itself?

Once the new DCOM security level in enabled on the OPC server, remote OPC clients that do not implement Packet Integrity Authentication Level will fail to connect to the OPC Server.

In our products, a test connection failure will show the following message in our client software:

> ***Create instance failed: 0x80070005***

In addition, the user should verify in the Windows event log of the client machine that this error is due to Packet Security Authentication Level:

- Run Windows Event Viewer
- Navigate to Windows Logs > System
- Look for a recent error for source “DistributedCOM”
- Example error message for our OPC client products:
    - ***Application xxx with PID yyy is requesting to activate CLSID {guid} on computer opcservermachinename with explicitly set authentication level at 2.***
      The lowest activation authentication level required by DCOM is 5(RPC_C_AUTHN_LEVEL_PKT_INTEGRITY).
      To raise the activation authentication level, please contact the application vendor.
- If this error message does not appear in the Windows event log of the client machine
    - If client machine updated with the June 8th, 2021 Windows security updates: the connection error is most likely not due to the new DCOM security level.
    - If client machine NOT updated with the June 8th, 2021 Windows security updates: the error message that appears may be
      DCOM got error "2148007941" from the computer opcservermachinename when attempting to activate the server

The Windows event log of the server machine will also log an error due to a client that does not implement Packet Security Authentication Level:

- Run Windows Event Viewer
- Navigate to Windows Logs > System
- Look for a recent error for source “DistributedCOM”
- Example error message in the server log:
    - ***The server-side authentication level policy does not allow the user domainname\username SID (sid) from address a.b.c.d to activate DCOM server.***
      Please raise the activation authentication level at least to RPC_C_AUTHN_LEVEL_PKT_INTEGRITY in client application.

How are Exele OPC client products affected by this change?

Our current release of OPC client products (as of December 2021) do not implement the required client security level “Packet Integrity”.

Using the steps outlined in KB5004442 we were able to create the connection failure to a remote OPC server with the RequireIntegrityActivationAuthenticationLevel registry key enabled.

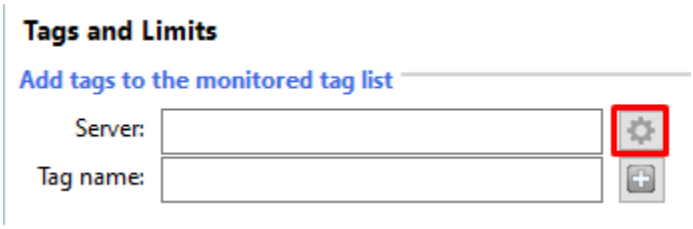
We were then able to update our internal code to support Packet Integrity level.

Am I using a local or remote OPC Server?

The new DCOM security level change does not affect connections to a local OPC Server on the same machine as the OPC client product.

To check the details of your OPC Server connection(s), launch the OPC Server Alias screen:

- **TopView**:
  - Launch the TopView Configurator
  - From the left menu select “Tags and Limits”
  - On the Tags and Limits screen click the gear icon to the right of the Server text box



- **OPCcalc**
  - Windows Start button > OPCcalc > OPC Server Alias Config
  - Click the [Edit Aliases] button

For each defined OPC Server Alias check the configured “Host computer” name.

For local OPC Servers, the “Host computer” should be blank/empty. You may also see “localhost” or the IP address of the local machine. For remote OPC Server, the “Host computer” will be the host name or IP address of the remote machine.

Patching existing Exele OPC Clients (TopView and OPCcalc)

Patching will be available for customers with an active Software Support Agreement. To obtain the patch users can send an email to support@exele.com requesting the DCOM security patch.

The patch can be applied to existing Exele OPC client products that meets the following criteria:

- OPC DA/HDA : Client product built with.Net Framework 4 or later
- OPC A&E: Client product built with .Net Framework 4.6.1 or later

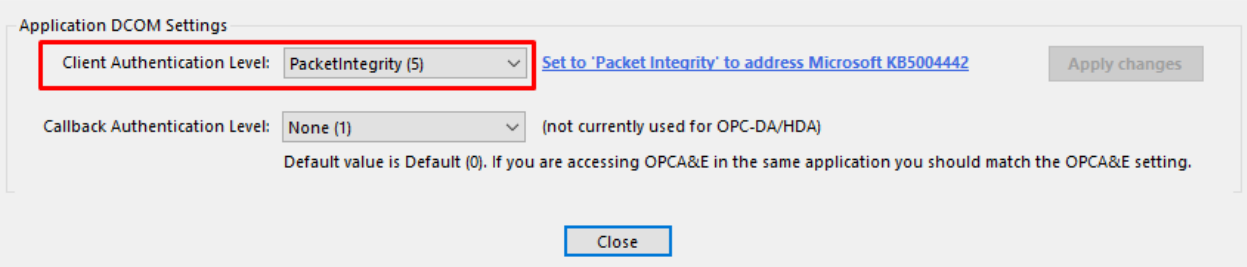
The patch can be applied to the following Exele OPC products:

- **TopView OPC/SCADA and OPC A&E version 6.25.3 and later**
- **OPCcalc versions 4.5 and 4.6**

The patch will be available through the following methods:

- TopView
    - An updated installation for TopView v6.36 will install the required patch files
    - If a user has version 6.36 installed they can
        - Install the updated installation package
        - Manually apply the patch files to their 6.36 installation
    - If a user has version 6.25.3 through 6.35 they can
        - Upgrade to 6.36 with the updated installation package
        - Manually apply the patch files to their current TopView version
- OPCcalc
    - If the user has version 4.5 or 4.6 they can manually apply the patch files
    - Users with earlier versions will need to upgrade and apply the patch files

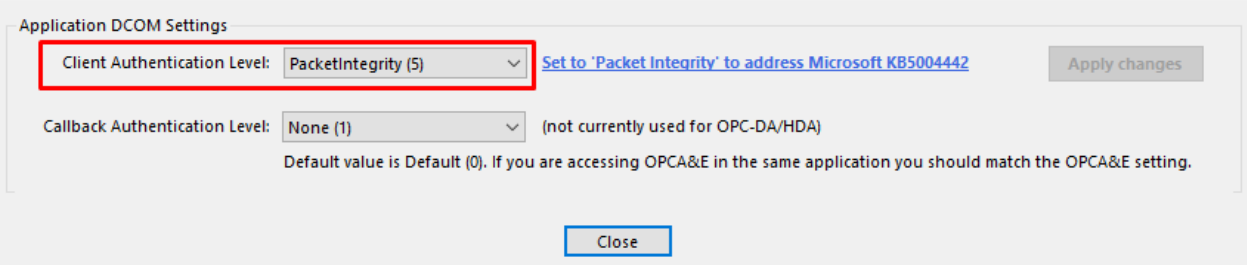
The required client DCOM security level will be enabled by default but can be changed on the bottom of the updated OPC Server Alias screen in TopView and OPCcalc.



Exele OPC Test Tool – updated with Packet Integrity

Our free OPC Test Tool has been updated with Packet Integrity authentication level. Users can download this tool to verify successful connection to remote OPC Servers that require Packet Integrity.

The required client DCOM security level will be enabled by default but can be changed on the bottom of the OPC Server Alias screen in the test tool.



If users are failing to connect to a remote OPC Server in TopView or OPCcalc due to the new DCOM security level, the Exele OPC Test Tool can be used to verify a successful connection before applying the patch.