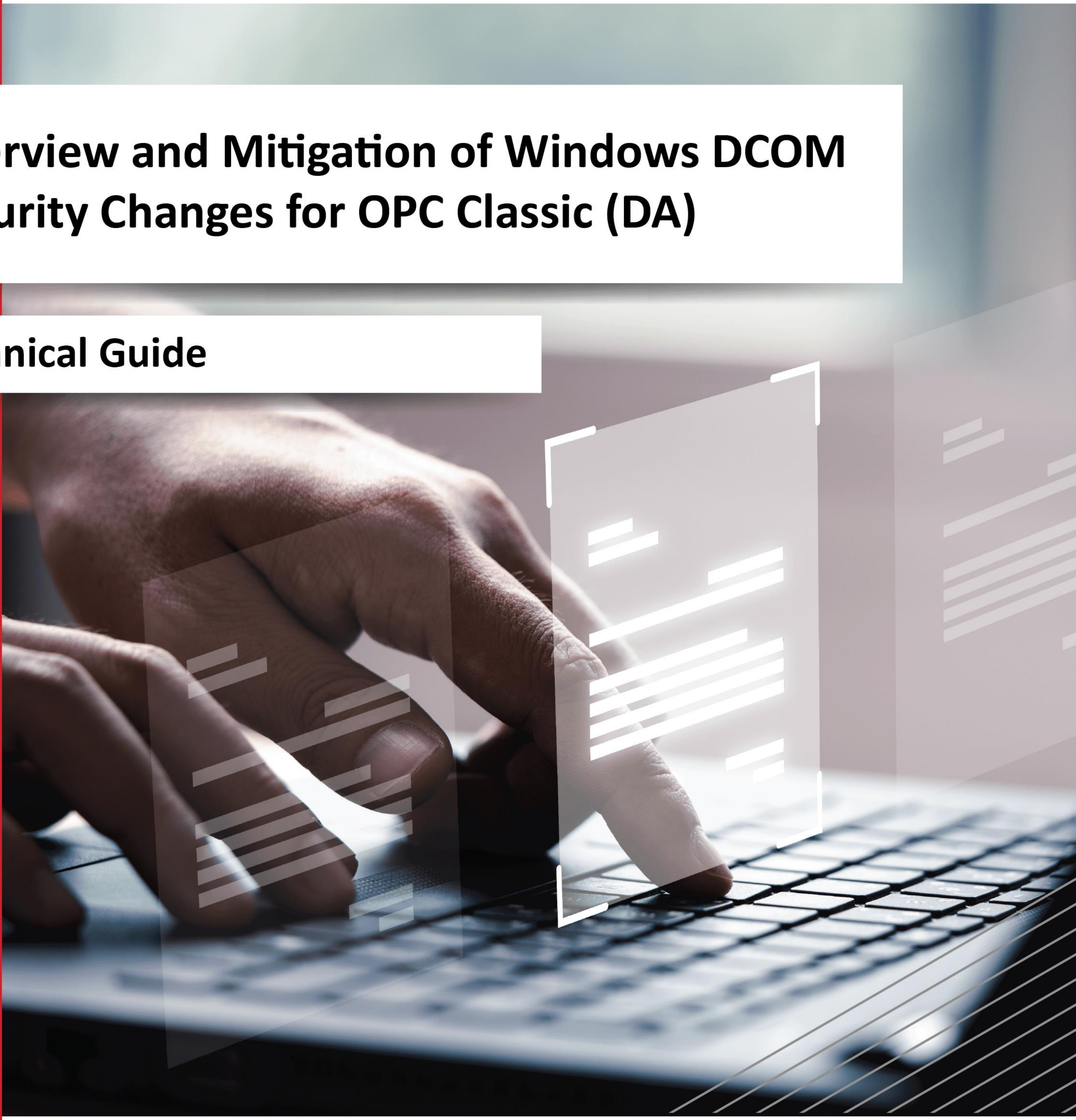
Industrial Data Xchange
The Industrial Data Communications Experts

# Overview and Mitigation of Windows DCOM Security Changes for OPC Classic (DA)

## Technical Guide



A summary of the changes and testing procedures required to ascertain whether OPC DA Client and Server applications will be compatible with the pending DCOM changes.

**What's covered in this guide:**
DCOM Authentication levels • Affected Operating Systems • Testing

# Contents

## 1. Introduction

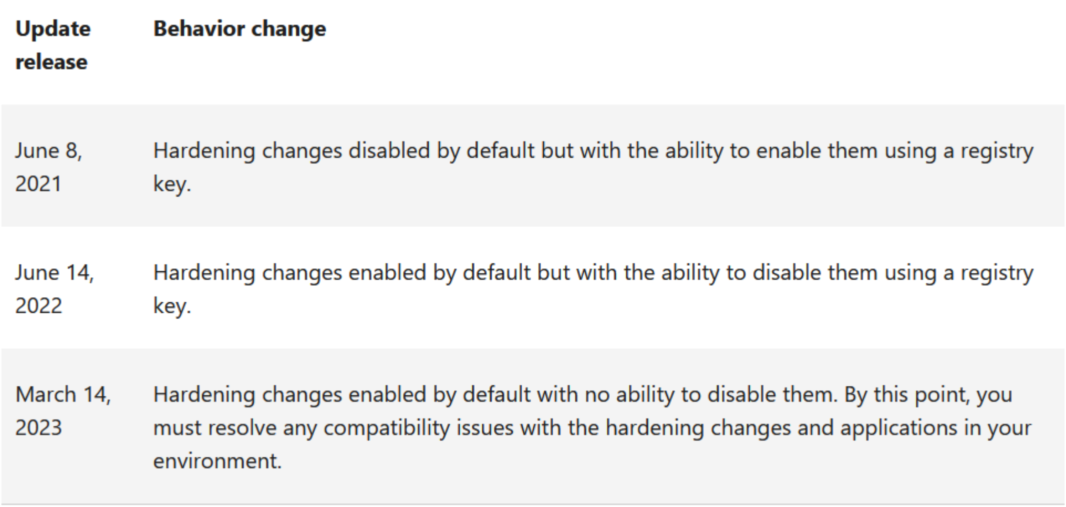
Distributed Component Object Model (DCOM) is an extension of the Component Object Model (COM) that allows COM components to communicate among objects on different computers. DCOM uses Remote Procedure Call (RPC) to generate standard packets that can be shared across a network, which in turn allows COM to communicate beyond the boundaries of the local machine.

Because DCOM poses a security threat, care should be taken to expose only what is required for the application. Although multiple security layers exist, it is still possible that some parts of the system can be compromised.

In 2021, Microsoft began the introduction of fundamental security changes to Windows DCOM to close identified security vulnerabilities (as described by https://support.microsoft.com/en-us/topic/kb5004442-manage-changes-for-windows-dcom-server-security-feature-bypass-cve-2021-26414-f1400b52-c141-43d2-941e-37ed901c769c).

The changes were introduced to increase the security of the communications between a DCOM client and server by introducing two new authentication mechanisms. These hardening changes have an implementation and mandatory enforcement timeline, meaning in Q1 2023, the DCOM Client/Server communication interface will require one of the new authentication levels to be used.

This means DCOM-dependent interfaces, such as those used by OPC DA, need to be compatible with and ready for the changes when they are enforced by the operation system, to ensure continued operation.



| Update release | Behavior change |
|---|---|
| June 8, 2021 | Hardening changes disabled by default but with the ability to enable them using a registry key. |
| June 14, 2022 | Hardening changes enabled by default but with the ability to disable them using a registry key. |
| March 14, 2023 | Hardening changes enabled by default with no ability to disable them. By this point, you must resolve any compatibility issues with the hardening changes and applications in your environment. |

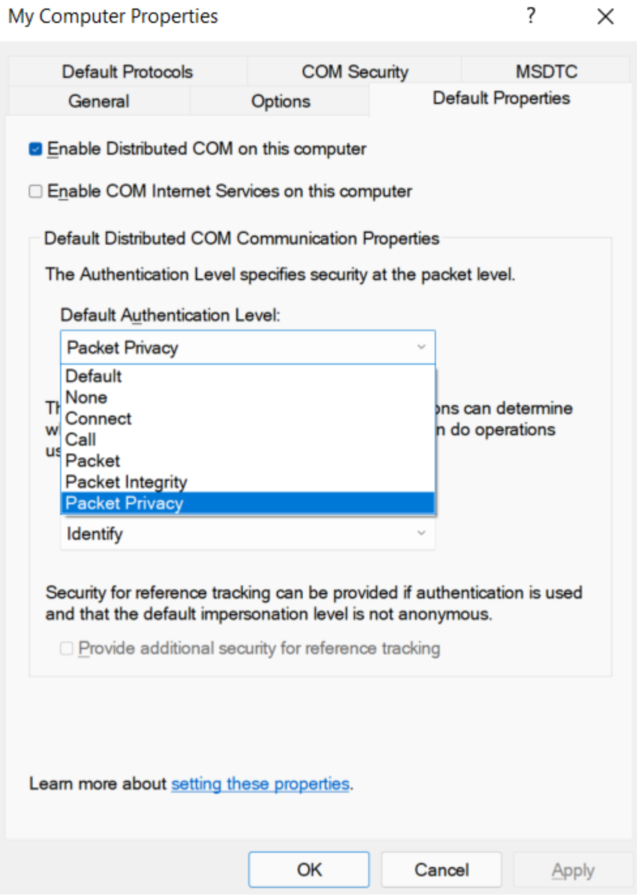
Figure 1: DCOM hardening deployment/enforcement schedule

This document provides a summary of the changes and testing procedures required to ascertain whether OPC DA Client and Server applications will be compatible with the pending DCOM changes.

## 2. DCOM authentication levels

The setting that the hardening involves is the DCOM authentication level. Currently, the authentication levels can be defined as:

- Default
- None
- Connect
- Call
- Packet
- Packet Integrity
- Packet Privacy



☑ Enable Distributed COM on this computer

☐ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level:

Packet Privacy

Identify

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

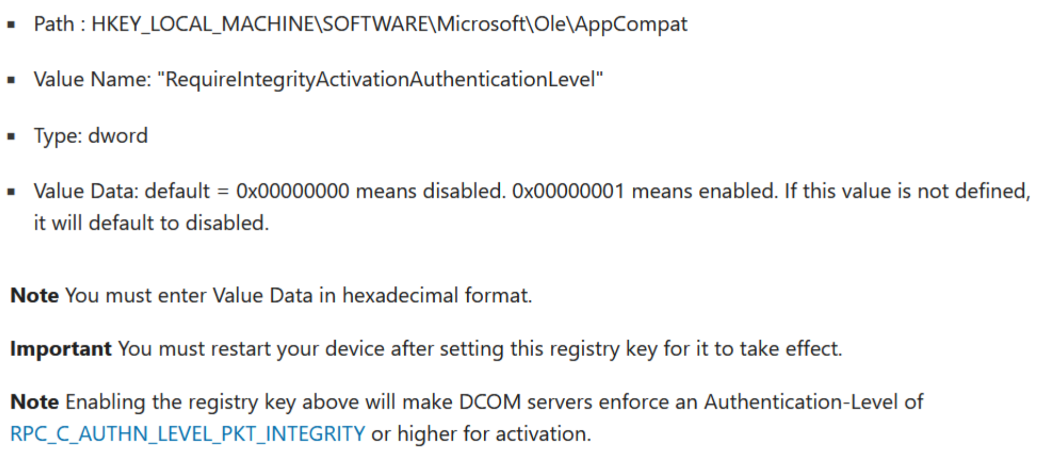
☐ Provide additional security for reference tracking

Learn more about setting these properties.

Figure 2: DCOM Authentical levels

By changing the default level for the system in the above dialogue, or per specific server instance, will require a connecting client to meet or exceed that authentication level when it attempts to connect to a server. As of Q1 2023, the operating system will enforce that all servers require at least the *Packet Integrity* level setting.

Until that date, if the security update has been applied, the registry setting as in *Figure 3* can be modified to enable or disable the OS-level enforcement of the authentication level. This setting will also enable logging to the event log of client connections that do not meet the required level.



- Path : HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole\AppCompat
- Value Name: "RequireIntegrityActivationAuthenticationLevel"
- Type: dword
- Value Data: default = 0x00000000 means disabled. 0x00000001 means enabled. If this value is not defined, it will default to disabled.

**Note** You must enter Value Data in hexadecimal format.

**Important** You must restart your device after setting this registry key for it to take effect.

**Note** Enabling the registry key above will make DCOM servers enforce an Authentication-Level of RPC_C_AUTHN_LEVEL_PKT_INTEGRITY or higher for activation.

Figure 3: Registry key to enable/disable OS level enforcement

A registered server will take on the system default DCOM authentication level. However, each server can have its DCOM authentication level defined and modified directly using the DCOMCNFG tool in Windows.

In addition, DCOM clients either use a default/negotiated DCOM authentication level or more often they define the DCOM authentication level they will use for connections which usually cannot be modified by an end-user.

Thus, clients are the OPC DA component primarily affected by these hardening changes as the internal authentication level used is often lower than the Packet Integrity level that will be enforced and requires code modification to make compliance with the Microsoft changes.

*Note that machine local OPC client/server OPC DA communication is not affected by this DCOM change.*

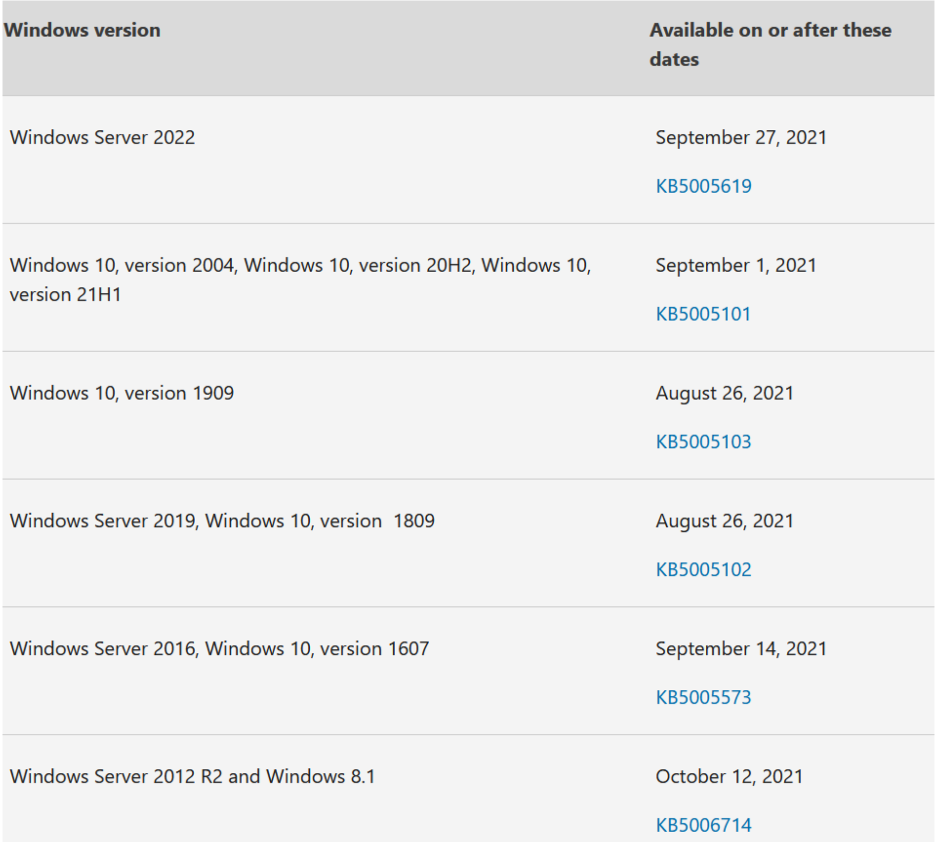
## 3. Operating Systems Affected

A security update that implements the hardening change was issued for a wide range of operating systems, even those that are no longer included in Microsoft’s normal update lifecycle. This includes:

- Server operating systems from Windows Server 2008 w/SP2
- Desktop operating systems from Windows 7 w/SP1

The full OS list is detailed on the vulnerability web page: (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-26414).

However, full error reporting via the Windows Event logs of communication that is blocked due to a non-compliant client is only provided on the following operating systems:



| Windows version | Available on or after these dates |
|---|---|
| Windows Server 2022 | September 27, 2021<br>KB5005619 |
| Windows 10, version 2004, Windows 10, version 20H2, Windows 10, version 21H1 | September 1, 2021<br>KB5005101 |
| Windows 10, version 1909 | August 26, 2021<br>KB5005103 |
| Windows Server 2019, Windows 10, version  1809 | August 26, 2021<br>KB5005102 |
| Windows Server 2016, Windows 10, version 1607 | September 14, 2021<br>KB5005573 |
| Windows Server 2012 R2 and Windows 8.1 | October 12, 2021<br>KB5006714 |

Figure 4: Windows OS versions that provide DCOM event logging related to the DCOM security changes.

## 4. Testing

The following steps can be used to identify non-compliant clients. Note that these steps should only be tested on non-production systems or when testing can be performed without affecting production as appropriate:

- On the server machine, edit the registry key as per Figure 3 to enable OS-level enforcement. The server will need to be restarted for the change to take effect.

- On the server machine, record the current authentication level before setting the default authentication level in the DCOMCNFG utility (My Computer -> Default Properties) to Packet Integrity, as per Figure 5. Note that on operating systems listed in Figure 4 with the requisite security update enabled, any failed client connections will cause an event log entry on the server similar to that shown in Figure 6.

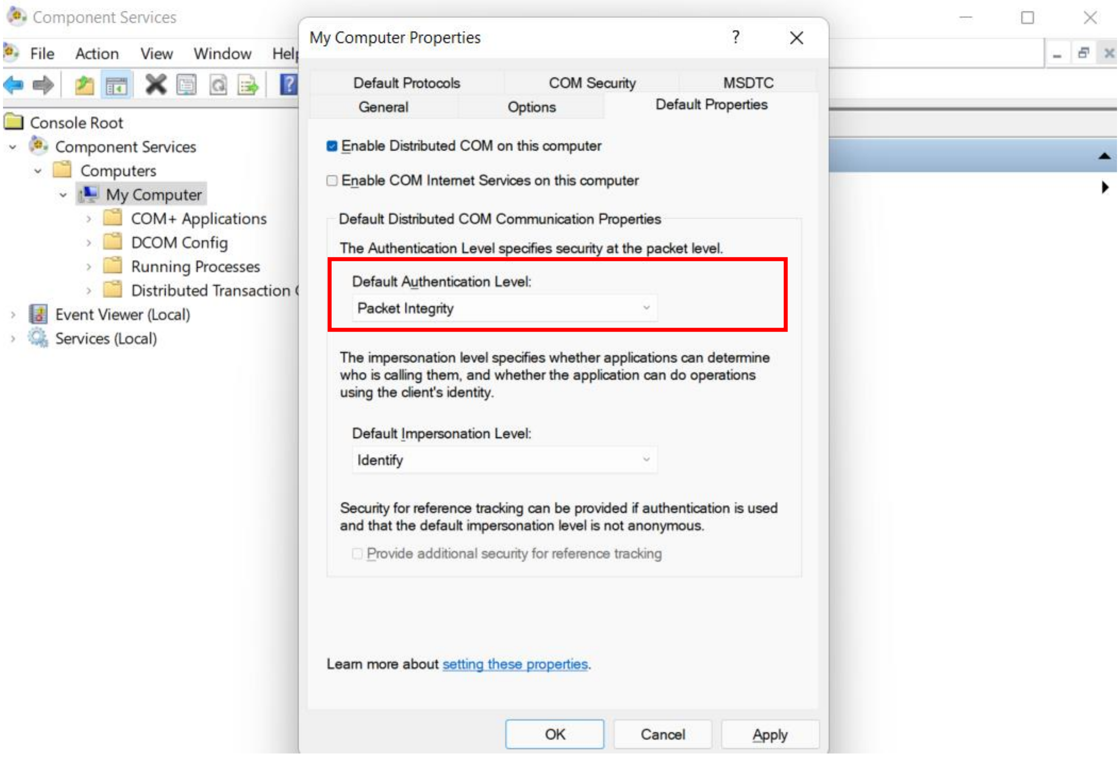
- On the server machine, check that the individual server instance DCOM settings are either using the default authentication level or manually changing the level to Packet Integrity, as per Figure 7. Note any changes made.

- Restart any client and server applications that were running a Windows service or were already open at the time the DCOM settings were changed.

- Verify that all the necessary clients can successfully browse/connect to the servers and that data updates are working correctly.

- For clients that are now unable to connect due to an Access Denied error, this is indicative of a client requesting a DCOM authentication level that is insufficient. Check the client & server machine System Event log for errors. An updated client will need to be obtained from the vendor that specifies a negotiated authentication level (RPC_C_AUTHN_LEVEL_DEFAULT) or uses Packet Integrity (RPC_C_AUTHN_LEVEL_PKT_INTEGRITY) as a minimum for the Authentication level parameter in the CoInitialiseSecurity API call. Alternatively, if supported by the server, an OPC UA client can be used instead.

- To undo the changes, revert the DCOM settings on the server to those recorded. Set the registry setting back to 0 and reboot the server.



☑ Enable Distributed COM on this computer

□ Enable COM Internet Services on this computer

Default Distributed COM Communication Properties

The Authentication Level specifies security at the packet level.

Default Authentication Level:
Packet Integrity

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

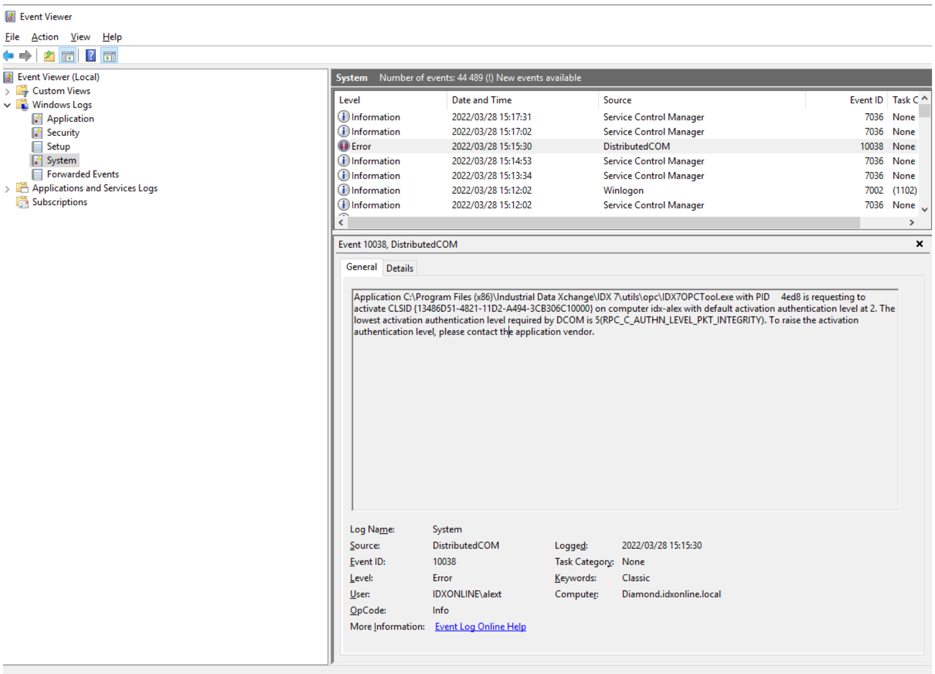
Default Impersonation Level:
Identify

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

□ Provide additional security for reference tracking

Learn more about setting these properties.

Figure 5: Default system authentication level



System Number of events: 44 489 (!) New events available

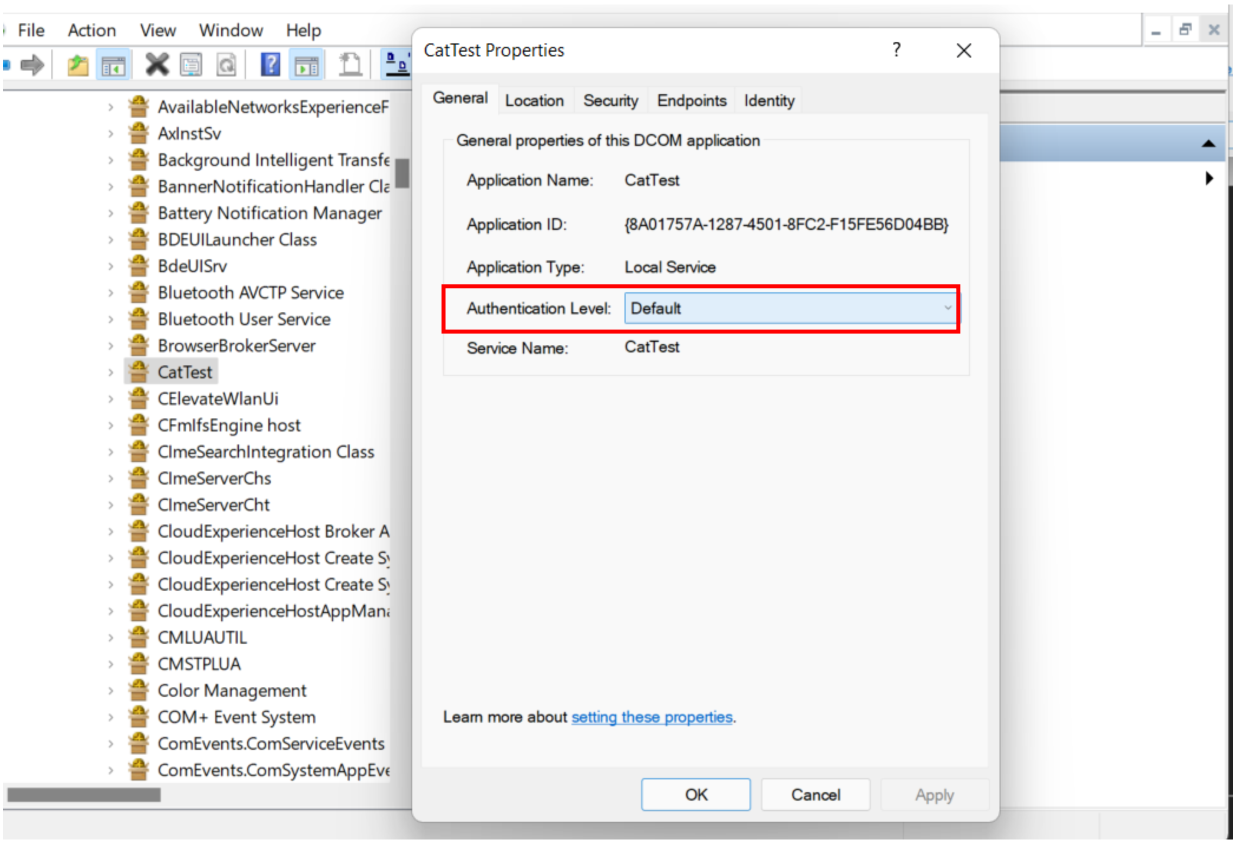
| Level | Date and Time | Source | Event ID | Task C |
|---|---|---|---|---|
| Information | 2022/03/28 15:17:31 | Service Control Manager | 7036 | None |
| Information | 2022/03/28 15:17:02 | Service Control Manager | 7036 | None |
| Error | 2022/03/28 15:15:30 | DistributedCOM | 10038 | None |
| Information | 2022/03/28 15:14:53 | Service Control Manager | 7036 | None |
| Information | 2022/03/28 15:13:34 | Service Control Manager | 7036 | None |
| Information | 2022/03/28 15:12:02 | Winlogon | 7002 | (1102) |
| Information | 2022/03/28 15:12:02 | Service Control Manager | 7036 | None |

Event 10038, DistributedCOM

```
Application C:\Program Files (x86)\Industrial Data Xchange\IDX 7\utils\opc\IDX7OPCTool.exe with PID    4ed8 is requesting to
activate CLSID {13486D51-4821-11D2-A494-3CB306C10000} on computer idx-alex with default activation 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.
```

| | | | |
|---|---|---|---|
| Log Name: | System | | |
| Source: | DistributedCOM | Logged: | 2022/03/28 15:15:30 |
| Event ID: | 10038 | Task Category: | None |
| Level: | Error | Keywords: | Classic |
| User: | IDXONLINE\alext | Computer: | Diamond.idxonline.local |
| OpCode: | Info | | |
| More Information: | Event Log Online Help | | |

Figure 6: Example of a failed DCOM client connection due to insufficient authentication level (level hard coded into a client)



General properties of this DCOM application

Application Name: CatTest

Application ID: {8A01757A-1287-4501-8FC2-F15FE56D04BB}

Application Type: Local Service

Authentication Level: Default

Service Name: CatTest

Learn more about setting these properties.

Figure 7: Individual OPC DA server DCOM authentication level

## 5. Conclusion

OPC is a powerful industrial communication standard. Nevertheless, OPC is dependent on having DCOM work properly. Fortunately, DCOM issues can usually be overcome with fairly simple configuration changes as detailed in this document.

To get a deeper understanding of OPC, we highly recommend that you take the time to get formal OPC training. This will enable you to structure your OPC knowledge to help you reduce your short and long-term project costs.

### About Industrial Data Xchange:

Industrial Data Xchange (IDX) is an Industrial and Communications Technology (ICT) Partner that provides industry-related products, services, solutions, and training. We assist you to establish, maintain and leverage connectivity within your infrastructure.

**Connectivity for Business Benefit:**
Address: 1 Weaver Street, Fourways, Johannesburg, Gauteng, South Africa
Phone: +27 11 548 9960 | Email: info@idx.co.za | Website: www.idx.co.za

IDX Industrial Data Xchange
The Industrial Data Communications Experts