Matrikon®
Powering Interoperability.

Datasheet

Matrikon OPC Security Gateway (OSG)

Version 3.1.5

Matrikon OPC Security Gateway secures 3rd party, real-time and historical, OPC Classic architectures. Unlike regular OPC solutions, which provide coarse DCOM-based security, OSG offers granular control over who can browse, add, read, and write to each OPC item on a per-user and per-tag basis on any OPC server.

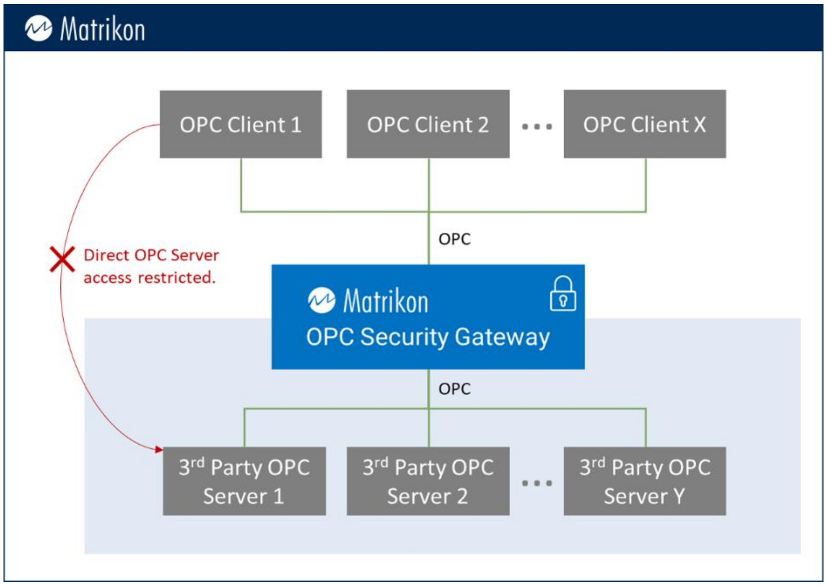
OSG is based on the OPC Foundation's OPC Security specification for maximum interoperability, making it an open standards-based solution. Use OSG to transform your OPC architectures from a security liability to an effective part of your defense-in-depth strategy.

Overview

OSG provides robust OPC DA server security integrated into a single application. Optional OPC HDA support is also available.

Key OSG highlights include:

- Universal compatibility with all OPC DA compliant clients and servers
- Multi OPC DA Server aggregation (federation)
- Selective OPC Server visibility to authorized users only
- Granular control over browse, read, and write operations
- OPC UA Tunneller ready – works directly with Matrikon OPC UA Tunneller client connections
- Role-based security
- Supports OPC DA Clients that do not support the OPC Foundation's OPC Security specification
- Non-disruptive setup enables existing systems to be secured without going offline
- Ties into existing Windows security
- OPC Foundation Security Specification compliance



Use Cases

OSG is used in a wide range of applications which include scenarios like:

- Per-user assignment of custom access rights to data from specific OPC servers.
- Granular control over actions each authorized user can do on a per OPC server and per-item basis. Controlled activities include item browsing, reading, and writing.
- Data source protection from potentially crippling loads generated by OPC client requests.
- Prevention of user-generated "device-writes" to control systems.
- OPC Client bulk item requests.
- Prevention of production data reads by unauthorized personnel. This is especially relevant in shared resource environments where contractors or partners should only access their portion of the overall address space.
- Securing OPC Servers that do not implement the OPC Security specification.
- Implementation of role-based security where different people require data access based on their roles.

Additional Features and Benefits

OPC HDA Support Option

OPC Security Gateway optionally supports OPC Historical Data Access (HDA). This option enables users to secure HDA OPC Servers with the following additional protection:

- Support for the following HDA operations:
  - Read Raw
  - Read Processed
  - Insert
  - Insert and Replace
- Secure OPC DA data passthrough from OPC HDA sources.
- Ability to expose raw data coming from underlying OPC Servers as processed data.
- Generation of multiple small data requests from a single large request. Throttling request size helps prevent overloading less performant OPC HDA Servers.
- Ability to throttle based on a maximum item count and maximum values per request.
- Reconnect and retry mechanism to handle request failures seamlessly.

OPC Alias Events Option

Create custom aliases for subscribed DA items and generate OPC Events on simple conditions including:

- Value Change
- Positive edge

Native Matrikon OPC UA Tunneller Support

For maximum security, OSG integrates natively with Matrikon OPC UA Tunneller for a total OPC security solution.

Benefits of pairing OSG with UAT include:

- OPC data protection via encryption
- Non-DCOM based connectivity
- Protection of source OPC Servers

OSG acts as a single-point-of-access to data from the OPC Servers it aggregates. Only authorized remote OPC Clients can browse and access data from aggregated OPC Servers via the (OSG) OPC Server.

Product Specifications

Supported Standards

OPC Specifications

- OPC Data Access Specification 2.05a
- OPC Data Access Specification 3.00
- OPC Historical Data Access Specification 1.2*
- OPC Alarms and Events Specification 1.10*
- OPC Security Specification 1.00

*Available via optionally licensed features

System Requirements

Hardware Requirements

The following PC Hardware is required:

- Intel® Pentium® 4 Processor
- 512 MB RAM
- 40 GB 7200 RPM Hard Drive

Supported Operating Systems

The following Windows Operating Systems will support this OPC Server:

- Microsoft Windows XP Pro SP3
- Microsoft Windows 2003 Server SP2 (32-bit and 64-bit
- Microsoft Windows 2008 SP2 (32-bit and 64-bit)
- Microsoft Windows 2008 Server R2 (64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows 10
- Microsoft Windows 2012
- Microsoft Windows 2016
- Microsoft Windows 2019

Matrikon
OPC Security Gateway

More Information

To learn more about Matrikon,

visit http://www.MatrikonOPC.com

or contact your Matrikon account manager.

Contact Information

sales@matrikonopc.com