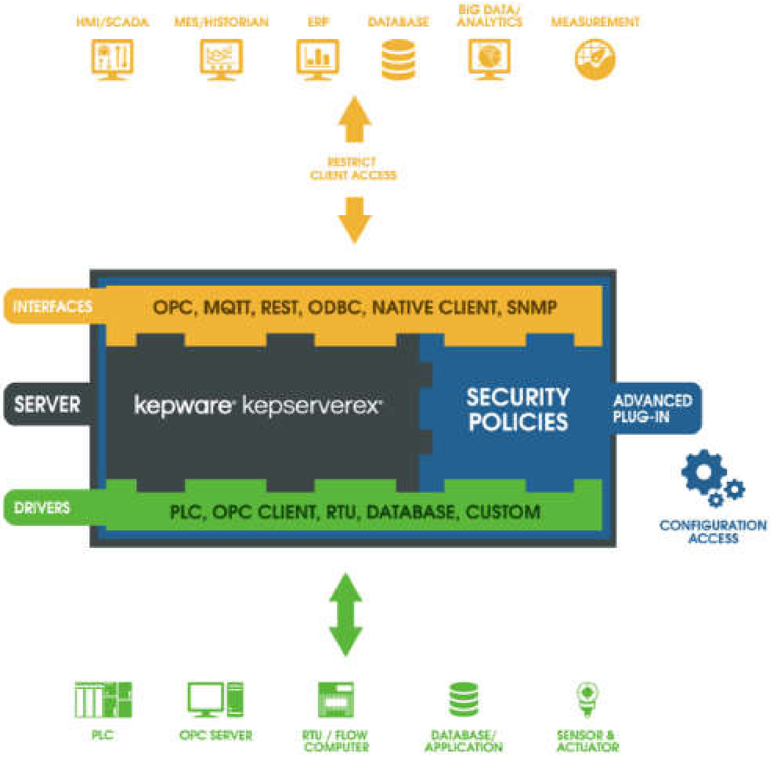
Security Policies Plug-in
SKU: KWP-SECPO0-PRD

Product Overview

The Security Policies advanced plug-in allows administrators to assign security access permissions on individual objects (such as channels, devices, and tags) based on the role of the user interacting with the Runtime project. It is used in conjunction with the server's User Manager, which enables management of user groups, users, and default security settings.



Features

- Allow and deny Dynamic Tag addressing
- Organize security policies by user groups
- Support for the following user group access categories:
  - Dynamic Addressing
  - I/O Tags
  - System Tags
  - Internal Tags
  - Browsing
- Support for the following user group permissions types:
  - Read
  - Write
  - Browse
- View and locate prior changes through the advanced plug-in interface’s font styling hierarchy and color scheme
- Copy permissions for the current access category to/from a user group
- Move permissions for the current access category to/from a user group
- Clear all custom permissions from an access category

ADDITIONAL TECH INFO

REQUIREMENTS AND RESTRICTIONS

- Client Application Support
  - User Level Support: OPC UA
  - Anonymous Login Support: OPC DA, OPC .NET, OPC AE, Wonderware SuiteLink, and GE IP NIO
- Project Files
  - Once security permissions have been applied in the Security Policies tab, the project can only be saved as a .opf file; .xml is no longer an option.
  - A project that contains security permissions will require Security Policies to be installed in order to load the file.