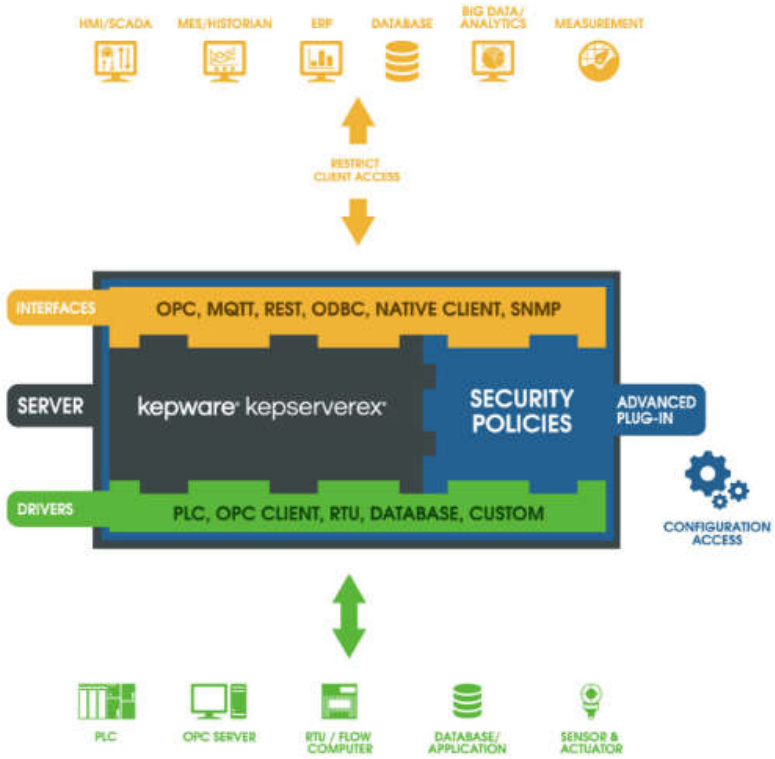
Security Policies Plug-in
SKU: KWP-SECPO0-PRD

Расширенный плагин Security Policies позволяет администраторам назначать права доступа к отдельным объектам (например, канал, устройств и тег) на основе роли пользователя, взаимодействующего с проектом во время его выполнения. Он используется в сочетании с сервером диспетчером пользователя, что позволяет управлять группами пользователей, пользователями и настройками безопасности по умолчанию.



Особенности

- Разрешает и запрещает динамическую адресацию тегов
- Организует политику безопасности для групп пользователей
- Поддерживает следующие категории доступа для групп пользователей:
  - Динамическая адресация
  - I/O Теги
  - Системные теги
  - Внутренние теги
  - Просмотр
- Поддерживает следующие разрешения для групп пользователей:
  - Чтение
  - Запись
  - Просмотр
- Просмотр и нахождение предыдущих изменений через расширенный интерфейс плагина, иерархия стиля шрифтов и цветовая схема
- Копировать разрешения для текущей категории доступа к/от группы пользователей
- Перемещать разрешения для текущей категории доступа к / от группы пользователей
- Очистить все пользовательские разрешения определенной категории доступа.

ДОПОЛНИТЕЛЬНАЯ ТЕХНИЧЕСКАЯ ИНФОРМАЦИЯ

ТРЕБОВАНИЯ И ОГРАНИЧЕНИЯ

- Поддержка клиентских приложений
  - Поддерживаемый уровень пользователей: OPC UA
  - Поддержка анонимного входа: OPC DA, OPC .NET, OPC AE, Wonderware SuiteLink, и GE IP NIO
- Файлы проекта
  - Когда разрешения безопасности были применены во вкладке Security Policies, проект может быть сохранен только в качестве .opf файла; файл.xml больше не доступен как опция.
  - Проект, который содержит разрешения безопасности, требует Security Policies, который должен быть установлен для того, чтобы загрузить файл.