الوحدات

جسر البيانات (بوابة IoT)

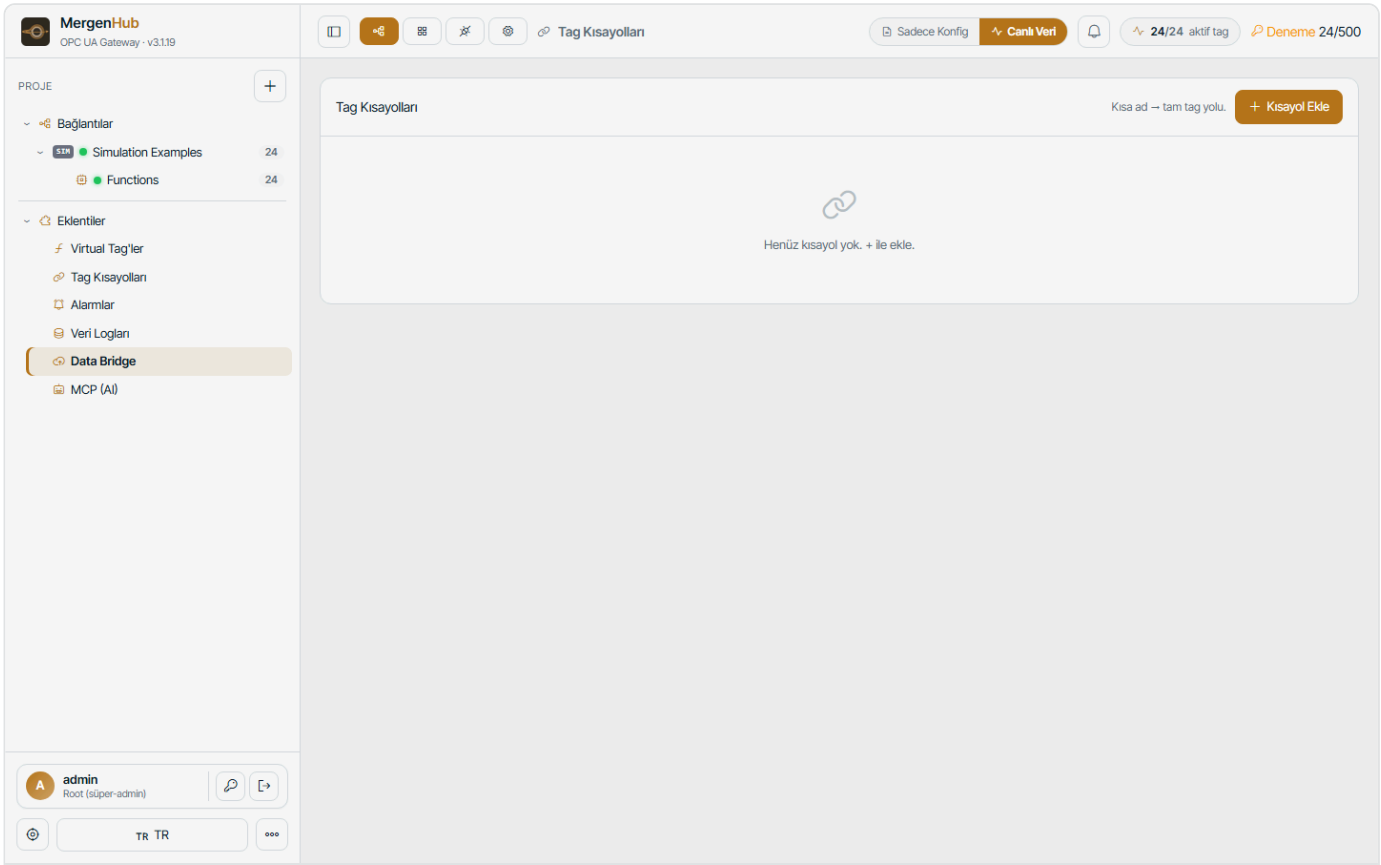
وكلاء خادم REST وعميل REST وعميل MQTT؛ صيغ الحمولة؛ نقاط نهاية متوافقة مع Kepware.

عبر الإنترنت: mergenhub.envest.com.tr/ar/docs/data-bridge

في هذه الصفحة

الوكلاء
الموثوقية
بدء سريع لـ REST server
ملاحظات أمنية
بدء سريع لـ MQTT client

ينقل جسر البيانات (Data Bridge، سابقًا IoT Gateway) البيانات **خارج** MergenHub إلى السحابات والوسطاء والأنظمة الخارجية، ويتيح لعملاء HTTP البسطاء قراءة الوسوم أو الكتابة إليها دون OPC UA. يعمل كخدمة Windows مستقلة (`MergenHubDataBridge`)، ولذلك لا يمكن لنقطة نهاية سحابية بطيئة أن تؤثر على المسح.



Extensions › Data Bridge — قائمة الوكلاء ومحرّر الوكيل

الوكلاء

الوكيل	الاتجاه	ما يفعله
REST server	وارد	نقاط نهاية HTTP متوافقة مع Kepware (`/iotgateway/read` و`/iotgateway/write` و`/iotgateway/browse`) بنفس صيغ JSON الخاصة بـ IoT Gateway من Kepware، فتعمل التكاملات الحالية دون تغيير
REST client	صادر	يدفع الوسوم المحددة إلى عنوان URL (POST/PUT) عند التغيّر أو وفق جدول؛ بصيغ JSON/XML/CSV/مفتاح-قيمة؛ مع ترويسات ومصادقة مخصّصة
MQTT client	صادر	ينشر الوسوم المحددة إلى وسيط (QoS وretain وTLS واسم مستخدم/كلمة مرور أو شهادة)؛ حمولات JSON، موضوع لكل وسم أو مجمّع؛ وقوالب اختيارية بنمط Sparkplug

لكل وكيل قائمة وسوم خاصة به، ومعدل نشر، ومرشّحات *عند التغيّر* / *النطاق الميت*، وصفحة حالة تعرض العدّادات وآخر خطأ.

بدء سريع لـ REST server

أضف وكيل *REST server*، واختر الوسوم، واسمح بالكتابة عند الحاجة. في الوكيل الجديد يكون الوصول المجهول معطَّلًا؛ ولا يفعّله إلا Root.

سجّل الدخول (ملف تعريف ارتباط الجلسة أو HTTP Basic) ثم اقرأ؛ ويجب أن يملك الحساب القارئ «الاتصال: عرض» ووصولًا إلى موارد الوسوم التي يقرؤها:

```
curl -b c.txt "http://localhost:8090/iotgateway/read?ids=Plant.PLC1.Flow&ids=Plant.PLC1.Pressure"
```

```
{"readResults":[{"id":"Plant.PLC1.Flow","s":true,"r":"","v":412.6,"t":1757067641008}, …]}
```

اكتب (عند تفعيل *allow write*؛ ويتطلب الحساب الكاتب «الكتابة إلى الوسوم والخدمات»):

```
curl -b c.txt -X POST http://localhost:8090/iotgateway/write -H "Content-Type: application/json" \
     -d '[{"id":"Plant.PLC1.Setpoint","v":55}]'
```

بدء سريع لـ MQTT client

الوسيط `mqtt://broker.example.com:1883` (أو `mqtts://` مع TLS)، ومعرّف العميل، وبيانات الاعتماد.

قالب موضوع مثل `plant/{channel}/{device}/{tag}` أو موضوع واحد بمصفوفة JSON.

وضع النشر: *عند التغيّر* (مع النطاق الميت) أو *كل N ms*.

مثال على الحمولة:

```
{"id":"Plant.PLC1.Flow","v":412.6,"q":"Good","t":"2026-09-05T10:20:41.008Z"}
```

الموثوقية

تخزّن الوكلاء البيانات مؤقتًا عند تعطّل الوجهة وتفرغها عند عودتها (تخزين وإعادة إرسال في الذاكرة بطابور محدود).

تعرض حالة الوكيل *متصل* / *إعادة المحاولة* ونص آخر خطأ؛ كما تُسجَّل الإخفاقات في سجل الأحداث.

ولأن الجسر عملية مستقلة، فإن إعادة تشغيله (*Settings › Services*) لا تقطع OPC UA ولا المسح.

ملاحظات أمنية

يستخدم REST server المستخدمين والصلاحيات والوصول إلى الموارد نفسها المستخدمة في API الرئيسي: القراءة تتطلب «الاتصال: عرض» والكتابة تتطلب «الكتابة إلى الوسوم والخدمات»؛ ولا تُعاد إلا الوسوم التي يحق للمستخدم قراءتها. الوصول المجهول معطَّل افتراضيًا ولا يفعّله إلا Root؛ وإذا كانت بيانات الاعتماد المقدَّمة غير صالحة فالردّ 401 حتى لو كان الوكيل في الوضع المجهول. وكل كتابة عبر هذه النقطة تُسجَّل في سجل التدقيق.

فضّل للأنظمة الخارجية HTTPS وحسابًا مستقلًا لا يصل إلا إلى الوسوم التي يحتاجها؛ ولا تعرّض منفذ الويب دون TLS أبدًا. ورؤية الوكلاء وإدارتها تتطلبان صلاحية «جسر البيانات».

MQTT: استخدم TLS وبيانات اعتماد لكل جهاز على الوسيط؛ ويتحقق MergenHub من شهادة الوسيط ما لم تعطّل ذلك لأغراض الاختبار.