الوحدات

المستخدمون والمجموعات والأمان

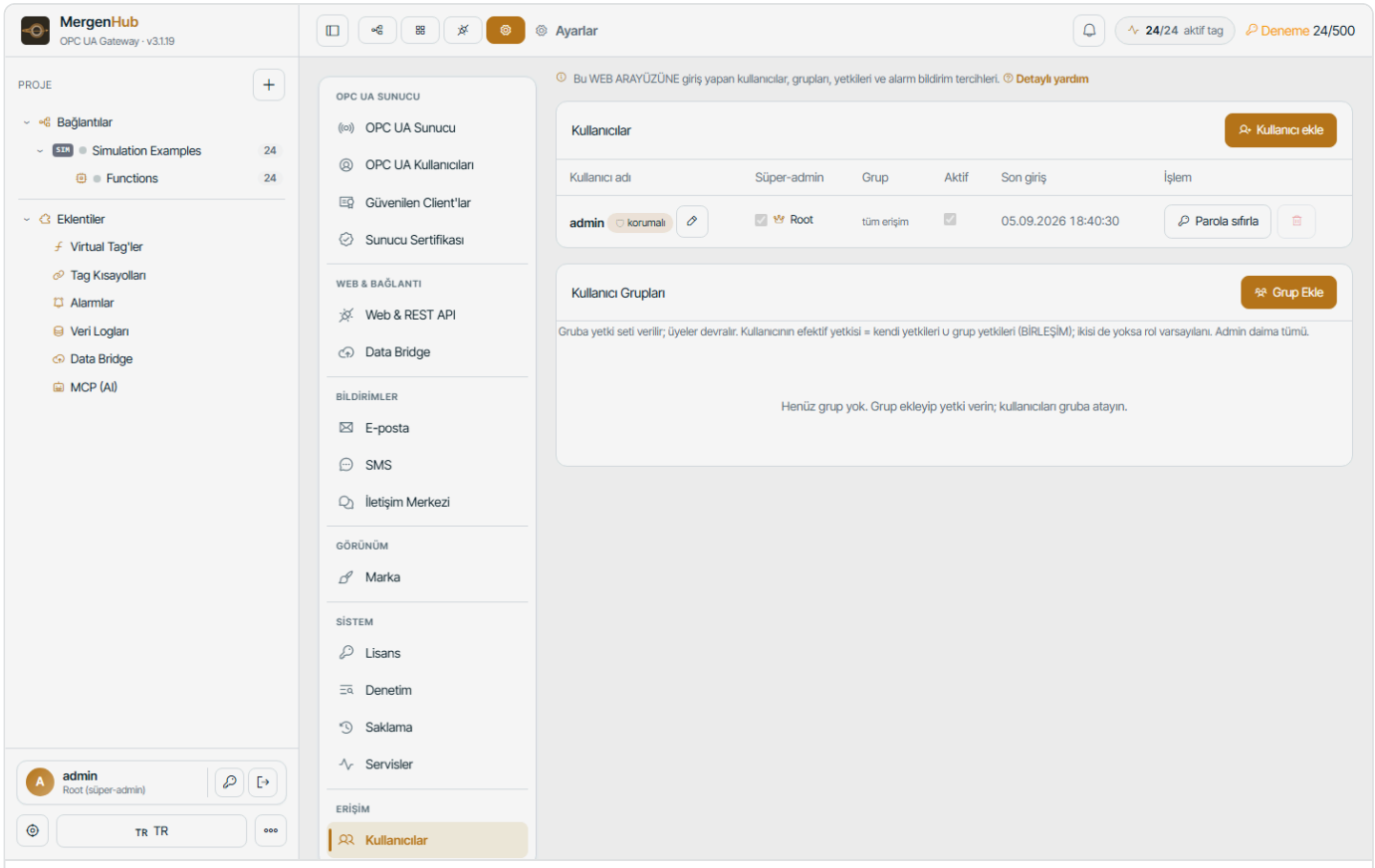
الأدوار والصلاحيات وقوائم التحكم بالموارد وHTTPS وسياسة الجلسات والتدقيق وقائمة التحصين.

عبر الإنترنت: mergenhub.envest.com.tr/ar/docs/users-security

في هذه الصفحة

الأدوار والصلاحيات
ACL للموارد
كلمات المرور والجلسات
HTTPS
أمان OPC UA
بيانات الاعتماد للسكربتات والأنظمة الخارجية
التدقيق
قائمة التحصين

يعتمد MergenHub نموذج مستخدمين واحدًا لواجهة الويب وREST API وOPC UA وجسر البيانات: **المستخدمون** ينتمون إلى **مجموعات**، وللمجموعات والمستخدمين **صلاحيات**، و**ACL للموارد** تحدد القنوات والأجهزة والمناطق التي يمكن لكل منهم رؤيتها أو الكتابة إليها.



الإعدادات › المستخدمون — الحسابات والمجموعات والصلاحيات

الأدوار والصلاحيات

لكل وحدة صلاحيتان منفصلتان: **عرض** و**إدارة** (31 صلاحية)؛ والإجراءات داخل الصلاحية (إضافة، تعديل، حذف، إقرار، تنزيل...؛ 91 إجراءً) يمكن تعطيلها واحدًا واحدًا للمستخدم أو للمجموعة. فمثلًا إقرار الإنذار يتطلب «الإنذارات: عرض»، وتغيير تعريف الإنذار يتطلب «الإنذارات: إدارة». التفاصيل والجدول المرجعي وأمثلة المصنع: الأدوار والصلاحيات.

لا يُختار الدور من الواجهة: صلاحيات الحساب تأتي من إعداد مسبق أو من مجموعته وتُضبط واحدةً واحدةً في نافذة الصلاحيات؛ وللمسؤول الأعلى يُؤشَّر مربع Root في قائمة المستخدمين.

الإعداد المسبق / الحساب	ماذا يفعل
الإعداد المسبق «مشاهد»	يرى الاتصال وSCADA والعدّادات والمقاييس وإدارة المياه والتقارير والأتمتة؛ ولا يغيّر شيئًا. لا إنذارات ولا سجلات بيانات ولا جسر بيانات ولا عميل OPC UA ولا مساعد ولا إعدادات. وكل حساب جديد يُنشأ من الواجهة يبدأ بهذه الصلاحيات
الإعداد المسبق «المشغّل»	يشغّل المنشأة (يكتب إلى الوسوم، ويقرّ الإنذارات، ويرى الوحدات)؛ ولا يغيّر أي تعريف
الإعداد المسبق «الصيانة»	إضافةً إلى الإعداد المسبق «المشغّل» يعرّف القنوات والأجهزة والوسوم ويصمّم الشاشات ويدير الوحدات؛ ولا يدخل إعدادات الخادم
الإعداد المسبق «المدير»	كل شيء بما فيه إعدادات الخادم، ما عدا الأعمال الخاصة بـ Root. وما يمنحه من صلاحيات وإجراءات يمكن تعطيله واحدًا واحدًا
Root (المسؤول الأعلى)	كل شيء. المستخدمون والمجموعات والوصول إلى الموارد والاحتفاظ والنسخ الاحتياطية وسجل الإصدارات وتصدير المشروع الكامل واستيراده مقصورة على Root

يحتفظ الخادم باسم دور لكل حساب (Viewer وOperator وAdming وRoot)؛ ولا يظهر Operator وAdming إلا في الحسابات المُنشأة في إصدار أقدم أو عبر REST. والحساب القديم الذي له دور المسؤول (Admin) كامل الصلاحيات دائمًا؛ وزر **إزالة الدور مع إبقاء الصلاحيات** في نافذة صلاحياته يجعله قابلًا للتقييد (التفاصيل).

تُقيَّم الصلاحيات مباشرة عند كل طلب — فتغيير حقوق المستخدم يسري فورًا دون إعادة تسجيل الدخول.

ACL للموارد

يمنح *Access ‹ Users ‹ Settings* المستخدمين أو المجموعات القنوات/الأجهزة/المناطق بصلاحية *قراءة* أو *قراءة+كتابة*. وهو **منع افتراضي** لغير Root: لا يرى المستخدم الجديد شيئًا إلى أن تُمنح له صلاحيات. تُسجَّل الملكية على الكائنات المنشأة ليحتفظ المنشئ بالوصول. تُطبَّق ACL على الواجهة وREST وOPC UA (تُصفّى مساحة العناوين) وجسر البيانات وMCP.

كلمات المرور والجلسات

سياسة كلمة المرور وفرض تغييرها عند أول تسجيل دخول (الافتراضي `admin/admin`).

تحديد معدل محاولات تسجيل الدخول (الرمز 429 بعد إخفاقات متكررة)، وتدقيق لعمليات تسجيل الدخول الناجحة والفاشلة.

سياسة الجلسات في *الإعدادات ‹ الويب وREST API والجوال*: مهلة الخمول، جلسة واحدة أو عدة جلسات لكل مستخدم، ملفات تعريف ارتباط آمنة (HTTPS).

نسيت كلمة المرور: رمز من 8 أرقام (صالح 5 دقائق) عبر البريد الإلكتروني أو الرسائل النصية عند ضبط وسيلة اتصال للمستخدم؛ ويمكن للمسؤولين إعادة الضبط من سطر الأوامر:

```
"C:\Program Files\MergenHub\MergenHub.exe" reset-admin "<new-password>" keep
```

HTTPS

راجع النشر على نطاق للشهادات والوكلاء العكسيين. عند تفعيل HTTPS يُعاد توجيه HTTP وتُوسَم ملفات تعريف الارتباط بأنها آمنة.

أمان OPC UA

نقاط نهاية بوضع Sign & Encrypt، والوصول المجهول معطّل، وقائمة العملاء الموثوقين، ووصول لكل مستخدم — راجع خادم OPC UA.

بيانات الاعتماد للسكربتات والأنظمة الخارجية

تُستدعى REST API بملف تعريف ارتباط الجلسة أو بـ HTTP Basic؛ ولا يوجد «رمز API» مستقل. تقرأ الأنظمة الخارجية التقارير **بمفتاح وصول إلى البيانات** (`mhkey_…`) لا يقرأ إلا التقارير؛ ويتصل عملاء الذكاء الاصطناعي برمز شخصي يُنشأ في صفحة **MCP (AI)**. وكلها تحمل صلاحيات مالكها وإجراءاته المعطَّلة ووصوله إلى الموارد؛ ويمكن حذف المفاتيح والرموز في أي وقت.

التدقيق

يُسجَّل كل تغيير في الكتابة وتسجيل الدخول والإعدادات مع المستخدم وعنوان IP والوقت (*Settings › Audit*)، ويُحفظ 90 يومًا افتراضيًا. راجع السجلات.

قائمة التحصين

[ ] غيّر كلمة مرور `admin` ؛ وأنشئ حسابات باسم كل شخص دون حسابات مشتركة

[ ] امنح المشغّلين الكتابة إلى الوسوم عند الحاجة فقط؛ وعطّل الإجراءات التي لا رجعة فيها مثل الحذف؛ وأبقِ Root لمالك النظام وحده (الأدوار والصلاحيات)

[ ] تفعيل HTTPS؛ وإعادة توجيه HTTP؛ وسياسة جلسات قوية

[ ] OPC UA: الوصول المجهول معطّل، وSign & Encrypt، وعملاء موثوقون فقط

[ ] جدار الحماية: المنافذ المطلوبة فقط، وشبكات مصدر مقيّدة (جدار الحماية)

[ ] راجع سجل التدقيق بشكل دوري؛ واحتفظ بنسخ احتياطية (النسخ الاحتياطي)