دليل المستخدم (داخل التطبيق، كامل)

الأمان والتفويض

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

في هذه الصفحة

الأدوار والصلاحيات: من يفعل ماذا وكيف تُمنح الصلاحيات
مرجع الإجراءات: ما الذي تتيحه كل صلاحية وكل إجراء
أمثلة من المصنع: أي المربعات لمن
الأسئلة الشائعة (الصلاحيات)
الصلاحيات صفحةً بصفحة: أي زر يتطلب أي صلاحية وأي إجراء
كلمات المرور و«نسيت كلمة المرور» والجلسات
HTTPS / النشر العام
تحصين الخادم: قفل مجلد البيانات، كلمة مرور النسخ الاحتياطي، تشفير القرص

الأدوار والصلاحيات: من يفعل ماذا وكيف تُمنح الصلاحيات

الإصدار 3.10.1

أربعة أمور تحدّد ما يستطيع المستخدم رؤيته وما يستطيع تغييره: كون الحساب **Root** أو لا، وصلاحيتا **عرض** / **إدارة** لكل وحدة، و**الإجراءات** التي يمكن تعطيلها واحدًا واحدًا داخل الصلاحية (إضافة، تعديل، حذف، إقرار، تنزيل…)، و**الوصول إلى الموارد** (أي القنوات والأجهزة والشاشات). المستخدم الذي لا يملك الصلاحية لا يرى الصفحة في القائمة إطلاقًا؛ والمستخدم الذي عُطِّل له إجراء لا يرى زرّه. والخادم يطبّق القاعدة نفسها عند كل طلب: فالإخفاء في الواجهة ليس الضمانة الوحيدة.

الموقع: **الإعدادات** ← **الوصول** ← **المستخدمون**. لا يرى هذا التبويب إلا حساب **Root** (المسؤول الأعلى). فيه بطاقتان: **المستخدمون** و**مجموعات المستخدمين**. زر **الصلاحيات** في صف المستخدم يفتح نافذة صلاحيات ذلك المستخدم، وزر **الصلاحيات** في صف المجموعة يفتح نافذة **صلاحيات المجموعة**؛ وكلتاهما المحرّر نفسه.

تتمة هذا الفصل مرجع الإجراءات: 31 صلاحية و95 إجراءً · أمثلة من المصنع · الأسئلة الشائعة · الصلاحيات صفحةً بصفحة

من يفعل ماذا: الجواب المختصر

لا يُختار الدور في هذه الواجهة. صلاحيات الحساب تأتي من **إعداد مسبق** أو من **مجموعته** وتُضبط واحدةً واحدةً في نافذة الصلاحيات؛ وللمسؤول الأعلى يُحدَّد مربع Root في قائمة المستخدمين. وباختصار فإن «الأدوار» ثلاثة أشياء: الإعدادات المسبقة الأربعة، و Root، ومجموعاتك أنت. وزر **؟** بجانب الشارة في قائمة المستخدمين وفي نافذة الصلاحيات وفي الملف الشخصي يفتح نافذة **الإعدادات المسبقة و Root** التي تشرحها.

الإعداد المسبق **مشاهد**. لمن يُمنح: من يكتفون بالمتابعة (المديرون والزوار ولوحات العرض). يرى شجرة المشروع والقيم الحيّة وشاشات SCADA والعدّادات وصفحات المياه والتقارير وتدفقات الأتمتة. لا يستطيع تغيير أي شيء ولا الكتابة إلى الوسوم؛ ولا يرى الإنذارات ولا سجلات البيانات. كل حساب جديد يُنشأ من الواجهة يبدأ بهذه الصلاحيات.

الإعداد المسبق **المشغّل**. لمن يُمنح: مشغّل الوردية. يشغّل المنشأة (يكتب إلى الوسوم، ويقرّ الإنذارات، ويرى الوحدات) لكنه لا يغيّر أي تعريف.

الإعداد المسبق **الصيانة**. لمن يُمنح: مسؤول الصيانة والأتمتة. إضافةً إلى الإعداد المسبق «المشغّل» يعرّف القنوات / الأجهزة / الوسوم ويصمّم الشاشات ويدير الوحدات. لا يستطيع دخول إعدادات الخادم.

الإعداد المسبق **المدير**. لمن يُمنح: مدير المنشأة أو تقنية المعلومات. كل شيء عدا الأعمال الخاصة بـ Root (بما فيه إعدادات الخادم). والصلاحيات والإجراءات الممنوحة بالإعداد المسبق يمكن تعطيلها لاحقًا واحدًا واحدًا.

Root (المسؤول الأعلى). يفعل كل شيء، إضافةً إلى الأعمال الخاصة بـ Root: المستخدمون والمجموعات، الوصول إلى الموارد، الاحتفاظ، الأمان، النسخ الاحتياطي، تصدير المشروع الكامل / استيراده، حذف سجلات التدقيق والأحداث. لمن يُمنح: مالك النظام. شخص واحد على الأقل وبضعة أشخاص على الأكثر؛ ولا يُستخدم للتشغيل اليومي. ويُمنح بمربع Root في قائمة المستخدمين.

المجموعات. أنشئ مجموعة لكل وظيفة في المنشأة (مثل: مشغّل الوردية، الصيانة، الطاقة): امنح الصلاحيات للمجموعة وعيّن المستخدم فيها. عند تغيّر الأشخاص تتغيّر عضوية المجموعة فقط؛ وتُدار الصلاحيات من مكان واحد.

> **إنشاء الحساب و Root** نافذة **إضافة مستخدم** تنشئ الحساب بصفة «مشاهد»؛ وإذا حُدِّد في النافذة مربع **المسؤول الأعلى (Root) — يدير المستخدمين والصلاحيات والوصول** صار الحساب Root. وفي القائمة يمنح المربع في عمود **المسؤول الأعلى** صفة Root لاحقًا أو يزيلها (يُكتب بجانب المربع **تعيين كـ Root** في الحساب غير Root و**Root** في حساب Root؛ عند إزالتها يصير الحساب «مشاهد»؛ ولا يمكن تنزيل آخر Root). والشارة تحت المربع تكتب دور الحساب: **مشاهد** أو **Root**. في الاستخدام اليومي لا حاجة إلى تغيير الدور: ما يفعله المستخدم تحدّده **مجموعته** ونافذة **الصلاحيات**.

> **الدور في الحسابات القديمة والحسابات المُنشأة عبر API** يحتفظ الخادم باسم دور لكل حساب (Viewer, Operator, Admin, Root). الحساب المُنشأ من الواجهة يكون Viewer أو Root؛ أما Operator و Admin فلا يظهران إلا في الحسابات المُنشأة في إصدار أقدم أو عبر REST (في الشارة: **المشغّل**، **المسؤول**). في نافذة صلاحيات حساب كهذا يظهر زر **إزالة الدور مع إبقاء الصلاحيات**؛ والتفاصيل أدناه تحت عنوان «الدور في الحسابات القديمة والحسابات المُنشأة عبر API».

كيف تعمل الصلاحيات: أربع طبقات

الطبقة	السؤال	أين تُضبط
1. Root	هل الحساب Root (المسؤول الأعلى) أم حساب عادي؟ Root يفعل كل شيء؛ أما ما يستطيعه الحساب العادي فيأتي من الطبقات الثلاث أدناه.	قائمة المستخدمين، عمود **المسؤول الأعلى**
2. الصلاحية (31 اسمًا)	أي وحدة **يراها** المستخدم وأي وحدة **يديرها**؟ الصلاحية هي باب الوحدة: من دون «عرض» لا تكون الصفحة في القائمة.	نافذة **الصلاحيات**: مربعات عرض / إدارة
3. الإجراء (95 اسمًا)	أي عمل لا يستطيعه في الوحدة التي يديرها (مثل: الحذف، الإقرار، التنزيل)؟ تُدار الإجراءات **بتعطيلها**: من ينال الصلاحية ينفّذ كل إجراءاتها، ثم يعطّل المسؤول ما يشاء منها.	نافذة **الصلاحيات**: زر **التفاصيل** في الصف
4. الوصول إلى الموارد	على أي قنوات وأجهزة ومناطق وشاشات يفعل ذلك؟	زر **الوصول** (في صف المستخدم أو المجموعة)

يُتحقَّق من الأربعة معًا: المستخدم الذي يملك «الإنذارات: عرض» وإجراء «إقرار الإنذارات» مفعّل لديه، لكنه لا يملك الوصول إلى وسم الإنذار، لا يرى ذلك الإنذار.

من أين تأتي الصلاحية

المصدر	ما يفعله
المجموعة (موصى به)	تُمنح المجموعة مجموعة صلاحيات وإجراءات معطَّلة فيرثها أعضاؤها. يُسنَد المستخدم إلى مجموعة من عمود **المجموعة** في قائمة المستخدمين. خمسة أشخاص يؤدّون العمل نفسه يُدارون من مكان واحد.
صلاحيات خاصة بالمستخدم	في نافذة **الصلاحيات** في صف المستخدم تُزيل علامة **دون صلاحيات خاصة (تسري صلاحيات المجموعة)** ثم تطبّق إعدادًا مسبقًا أو تحدّد المربعات واحدًا واحدًا. المستخدم ذو الصلاحيات الخاصة تظهر على زرّه نقطة صغيرة.
إن لم يوجد أيٌّ منهما	إذا لم تكن للمستخدم مجموعة ولا صلاحيات خاصة عمل الحساب بصلاحيات الإعداد المسبق «مشاهد». أما الحساب القديم أو المُنشأ عبر API بدور «المشغّل» أو «المسؤول» فتسري عليه مجموعة صلاحيات الدور (أدناه، «الدور في الحسابات القديمة والحسابات المُنشأة عبر API»).

كيف يجتمع المستخدم ومجموعته

الصلاحيات تتّحد. إذا كانت للمستخدم صلاحيات خاصة ومجموعة معًا سرى اتحاد الاثنتين: يكفي وجود الصلاحية في إحداهما.

المستخدم المنتمي إلى مجموعة وبلا صلاحيات خاصة تسري عليه المجموعة وحدها. صلاحيات البداية للحساب الذي لا مجموعة له (الإعداد المسبق «مشاهد») لا تُضاف إلى المجموعة؛ وليس للمستخدم ملف صلاحيات خاص به.

الإجراءات تتّحد أيضًا. يمكن تنفيذ الإجراء إذا سمح به مصدر واحد على الأقل. ولذلك **يبقى الإجراء المعطَّل لدى المستخدم مفعّلًا إذا كانت مجموعته تمنح الصلاحية نفسها بلا قيد**. ولتعطيل إجراء فعلًا عطّله في المجموعة أيضًا أو أخرج المستخدم من المجموعة.

المستخدم المنتمي إلى مجموعة وبلا صلاحيات خاصة يُمنح قيد الإجراءات لمجموعته. في نافذة صلاحيات هذا المستخدم تكون مربعات الإجراءات مقفلة وتعرض قيود المجموعة؛ وتظهر في الأعلى هذه الملاحظة: «ليست لهذا المستخدم مجموعة صلاحيات خاصة به؛ فصلاحياته تأتي من المجموعة «...». لتعطيل إجراءات لهذا المستخدم وحده أزل علامة «دون صلاحيات خاصة» أو عدّل صلاحيات المجموعة.» أما المستخدم الذي لا مجموعة له فيمكن تعطيل الإجراءات له والمربع محدَّد أيضًا (وتبقى مربعات عرض / إدارة مقفلة).

الحساب القديم بدور المسؤول (Admin) كامل الصلاحيات دائمًا. حتى لو أُزيلت علامات مربعات الصلاحيات أو عُطِّلت إجراءات فإنه ينفّذها كلها؛ ومربعات الإجراءات مقفلة. والنافذة تذكر ذلك: «هذا الحساب بدور المسؤول (Admin) وهو كامل الصلاحيات دائمًا. لتقييده اضغط زر «إزالة الدور مع إبقاء الصلاحيات».» الزر يحوّل الحساب إلى دور «مشاهد» ويحفظ صلاحياته الحالية صلاحياتٍ خاصة: فلا يتغيّر وصوله، ويصبح تعطيل الصلاحيات والإجراءات واحدًا واحدًا ممكنًا. ولا حاجة إلى دور لمدير جديد: يُستخدم الإعداد المسبق **المدير** أو مجموعة.

الرؤية ليست إجراءً مستقلًا. الصلاحية نفسها هي دخول الوحدة ورؤيتها. المستخدم الذي عُطِّلت كل إجراءاته يظل يرى الوحدة؛ وإن أُريد ألّا يراها أُزيلت علامة مربع «عرض».

الإجراء الجديد يأتي مفعّلًا. لأن المحفوظ هو قائمة الإجراءات المعطَّلة، فإن أي إجراء يُضاف مستقبلًا يكون مفعّلًا تلقائيًا لكل من يملك صلاحيته الأم؛ فلا يفقد أحد وصوله عند الترقية.

التغيير يسري فورًا. تُحسب الصلاحيات والقيود من جديد عند كل طلب؛ ولا يحتاج المستخدم إلى الخروج والدخول. وكل تغيير يُكتب في سجل التدقيق (مَن، ولمن، الصلاحيات المضافة / المزالة، الإجراءات المعطَّلة / المفعَّلة).

القاعدة نفسها في كل طريق دخول. واجهة الويب و REST API وتطبيق الجوال ومفتاح الوصول إلى البيانات ورمز MCP الخارجي والمساعد داخل التطبيق تمرّ كلها بمجموعة الصلاحيات والإجراءات نفسها.

نافذة الصلاحيات خطوة بخطوة

افتح النافذة. الإعدادات ← الوصول ← المستخدمون؛ ثم **الصلاحيات** في صف المستخدم أو المجموعة. في نافذة المستخدم يظهر في الأعلى **اسم المستخدم**، وبجانبه الشارة وزر **؟** ومجموعته إن وُجدت؛ وتحته التلميح «يمكنك منح صلاحيات لهذا المستخدم أو سحبها؛ وتُجمع مع صلاحيات مجموعته.» ومربع **دون صلاحيات خاصة (تسري صلاحيات المجموعة)**. ما دام المربع محدّدًا فليست للمستخدم صلاحيات خاصة وتُعرض مربعات عرض / إدارة عرضًا فقط (صلاحيات المجموعة للمستخدم المنتمي إلى مجموعة؛ وصلاحيات الإعداد المسبق «مشاهد» لمن لا مجموعة له). وإذا كان الحساب بدور قديم «المشغّل» أو «المسؤول» ظهر تحت التلميح سطر معلومات وزر **إزالة الدور مع إبقاء الصلاحيات** أيضًا.

اختر نقطة البداية. عند إزالة علامة **دون صلاحيات خاصة (تسري صلاحيات المجموعة)** يظهر سطر **إعداد مسبق (انقر ← ثم اضبط بدقة):** وفيه: **مشاهد**، **المشغّل**، **الصيانة**، **المدير**. الإعداد المسبق يملأ المربعات بنقرة واحدة و**يمسح قيود الإجراءات**. وإن وُجد مستخدم أو مجموعة مشابهة فاختره من قائمة **نسخ من مستخدم آخر / مجموعة أخرى...**: تُنسخ صلاحياته وإجراءاته المعطَّلة (عند النسخ من مستخدم يؤخذ ما يستطيعه فعليًا مع مجموعته).

حدّد مربعات عرض / إدارة. تتكوّن النافذة من ثلاثة أقسام: **الوحدات** (كل صف وحدة، وفيه عمودان: عرض وإدارة؛ والأزرار **عرض الكل**، **إدارة الكل**، **مسح**)، و**العمليات والأدوات** و**النظام** (الزرّان **الكل**، **بلا**). عند تحديد «إدارة» يُحدَّد «عرض» تلقائيًا؛ وعند إزالة «عرض» تُزال «إدارة» أيضًا. في صف **جسر البيانات** مربع واحد (**عرض وإدارة**). وسطر المعلومات أسفل قسم النظام يعدّد الصلاحيات الموجودة لدى Root فقط.

عطّل الإجراءات. زر **التفاصيل** في يمين الصف يفتح إجراءات تلك الصلاحية. الكائنات مثل القنوات والأجهزة والوسوم تُعرض في شبكة: الصف هو الكائن، والأعمدة **إضافة**، **تعديل**، **حذف**. أما الإجراءات الأخرى فمربعات منفردة («إقرار الإنذارات»، «تنزيل التقارير»، «الكتابة إلى الوسوم»...). إزالة علامة المربع تعطّل الإجراء. مربع الصلاحية التي عُطِّل منها إجراء يظهر **جزئيًا** (بشرطة) وتظهر في الصف شارة على هيئة **مقيَّدة: عدد الإجراءات المعطَّلة 2**. وإذا أُزيلت علامة مربع الصلاحية حُذفت قيود تلك الصلاحية أيضًا.

ابحث وصفِّ. عند الكتابة في المربع العلوي («ابحث عن صلاحية أو إجراء (مثل: إنذار، حذف)...») تبقى الصفوف المطابقة فقط؛ وإذا كانت الكلمة اسم إجراء فُتحت تفاصيل الصف وظهرت تلك الإجراءات وحدها. ومربع **إظهار المعطَّل فقط** يسرد الصفوف التي عُطِّلت منها إجراءات والإجراءات المعطَّلة.

اقرأ الملخّص. في أسفل النافذة مربعان: **يستطيع** و**لا يستطيع**. يكتبان بلغة بسيطة وحدةً وحدة («الإنذارات: يرى; إقرار الإنذارات»، «الإنذارات: لا يدير (لا إضافة ولا تعديل ولا حذف)»). وإذا كانت للمستخدم مجموعة عدَّ الملخّص ما تمنحه المجموعة أيضًا ووسمه بعبارة **(من المجموعة)**: فإن بقي إجراء عطّلته لدى المستخدم في مربع «يستطيع» مع «(من المجموعة)» فالمجموعة هي التي تسمح به. وفي نافذة المجموعة يكون العنوان «أعضاء هذه المجموعة (بقدر ما تمنحه المجموعة)».

احفظ. حفظ. في قائمة المستخدمين يظهر تحت الاسم ملخّص من سطر واحد: «الإنذارات: إدارة (حذف تعريف الإنذار معطّل), SCADA: عرض +5»؛ ويُقرأ كاملًا بتمرير المؤشر فوقه. وفي الحساب القديم بدور المسؤول (Admin) يُكتب «المسؤول: كامل الصلاحيات». وفي قائمة المجموعات يظهر الملخّص نفسه على هيئة وسوم صغيرة.

المساعدة	أين	ما تعرضه
? الشارة والإعداد المسبق	بجانب الشارة (قائمة المستخدمين، نافذة الصلاحيات، الملف الشخصي)، وسطر الإعدادات المسبقة، وعنوان **صلاحياتي** في الملف الشخصي؛ والثلاثة تفتح النافذة نفسها	**الإعدادات المسبقة و Root**: جدول **محتوى الإعدادات المسبقة** (الصف وحدة أو صلاحية، والعمود إعداد مسبق)، و**لمن يُمنح** و**لا يستطيع** لكل إعداد مسبق، و Root، واقتراح المجموعات (**اقتراح**)، وفي الأسفل ملاحظة **الدور في الحسابات القديمة والحسابات المُنشأة عبر API**.
? الصف	كل صف وحدة أو صلاحية	وصف الصلاحية، ومثال، وجدول **الإجراءات ضمن هذه الصلاحية**.
? الإجراء	كل مربع إجراء في التفاصيل	ما يتيحه الإجراء، وما يحدث عند تعطيله، وضمن أي صلاحية يقع.
مساعدة	الشريط السفلي للنافذة	بطاقة ملخّص قصيرة عن المستخدمين والمجموعات.

في أسفل كل نافذة **?** رابطان: **الدليل المفصّل** يفتح هذا القسم، و**فتح في الموقع** يعرض المحتوى نفسه في وثيقة «الأدوار والصلاحيات» في الموقع.

> **صلاحياتي** يرى كل مستخدم عنوان **صلاحياتي** في النافذة التي تُفتح بزر **ملفي الشخصي** (أيقونة الشخص) بجانب اسمه: ملخّص الصلاحيات، وبجانبه **?** (نافذة «الإعدادات المسبقة و Root»)، وسطر **ما الذي أستطيع فعله وما الذي لا أستطيعه؟** (مربعا يستطيع / لا يستطيع). هذا أول مكان يُنظر فيه حين يقول مستخدم «لا أرى زرًّا ما».

إذا أبلغ الخادم عن صلاحية جديدة لا تعرفها الواجهة ظهرت في آخر النافذة تحت عنوان **أخرى** باسمها، ويمكن تحديدها كذلك.

الإعدادات المسبقة

الإعداد المسبق	ما يحدّده
مشاهد	عرض: الاتصال، SCADA، العدّادات والمقاييس، إدارة المياه، التقارير، الأتمتة. بلا أي «إدارة» وبلا أي عملية أو أداة وبلا أي صلاحية نظام. وبلا الإنذارات وسجلات البيانات كذلك.
المشغّل	مشاهد + الإنذارات: عرض (متابعة وإقرار)، سجلات البيانات: عرض، الكتابة إلى الوسوم والخدمات، عميل OPC UA، مساعد الذكاء الاصطناعي. لا يستطيع تغيير أي تعريف (بلا «إدارة»).
الصيانة	المشغّل + «إدارة» في كل الوحدات، جسر البيانات، القوالب والاستيراد، MCP، الشهادات، جدار الحماية، سجل التدقيق. بلا إعدادات الخادم وبلا إعدادات الإشعارات.
المدير	كل ما في النافذة عدا تنفيذ السكربتات.

الإعداد المسبق نقطة بداية: بعد تطبيقه تغيّر المربعات واحدًا واحدًا وتعطّل الإجراءات عبر **التفاصيل**. والإعداد المسبق «المشغّل» ليس هو **دور** «المشغّل» (Operator) في الحسابات القديمة: فالإعداد المسبق لا يغيّر أي تعريف، أما الدور فيدير كل الوحدات (الجدول أدناه).

الدور في الحسابات القديمة والحسابات المُنشأة عبر API

يحتفظ الخادم باسم دور لكل حساب (Viewer, Operator, Admin, Root). الحساب المُنشأ من الواجهة يكون Viewer أو Root؛ أما Operator و Admin فلا يظهران إلا في الحسابات المُنشأة في إصدار أقدم أو عبر REST. والشارة تكتب اسم الدور بلغة الواجهة. والدور يحدّد مجموعة الصلاحيات السارية ما دام الحساب بلا مجموعة وبلا صلاحيات خاصة:

الشارة (الاسم في الخادم)	بلا مجموعة وبلا صلاحيات خاصة	ملاحظة
مشاهد (Viewer)	مثل الإعداد المسبق «مشاهد»: يرى الاتصال و SCADA والعدّادات والمقاييس وإدارة المياه والتقارير والأتمتة. بلا الإنذارات وسجلات البيانات وجسر البيانات وعميل OPC UA والمساعد والإعدادات.	كل حساب جديد يُنشأ من الواجهة يبدأ بهذا الدور. تُمنح الصلاحيات من إعداد مسبق أو من مجموعة، ثم تُضبط واحدةً واحدةً في نافذة الصلاحيات.
المشغّل (Operator)	«عرض» و«إدارة» في كل الوحدات، جسر البيانات، الكتابة إلى الوسوم والخدمات، عميل OPC UA، القوالب والاستيراد، مساعد الذكاء الاصطناعي، MCP، سجل التدقيق. بلا إعدادات الخادم وإعدادات الإشعارات والشهادات وجدار الحماية.	يوجد فقط في الحسابات المُنشأة في إصدار أقدم أو عبر REST. وإذا كانت للحساب مجموعة أو صلاحيات خاصة فهي التي تسري. وللحساب الجديد يُستخدم إعداد مسبق أو مجموعة للنطاق نفسه.
المسؤول (Admin)	كل شيء عدا الأعمال الخاصة بـ Root وتنفيذ السكربتات.	يوجد فقط في الحسابات المُنشأة في إصدار أقدم أو عبر REST. لا يمكن تضييق هذا الدور: لا تُطبَّق عليه مربعات الصلاحيات ولا المجموعة ولا قيود الإجراءات. لتقييده: **إزالة الدور مع إبقاء الصلاحيات**.
Root (المسؤول الأعلى)	كل شيء.	يُمنح بالمربع في عمود **المسؤول الأعلى** في قائمة المستخدمين؛ ولا يمكن تنزيل آخر Root.

إزالة الدور مع إبقاء الصلاحيات: إذا كان دور الحساب «المشغّل» أو «المسؤول» ظهر في نافذة الصلاحيات، تحت التلميح، سطر معلومات وهذا الزر. ولا يوجد الزر في حساب «مشاهد» ولا في حساب Root.

اضغط **الصلاحيات** في صف المستخدم، ثم زر **إزالة الدور مع إبقاء الصلاحيات** في النافذة، وأكّد السؤال.

تُحفظ صلاحيات الحساب الحالية صلاحياتٍ خاصة، ثم يُحوَّل الحساب إلى دور «مشاهد». ولا يتغيّر وصوله. تظهر رسالة «أُزيل الدور؛ وأُبقيت الصلاحيات صلاحياتٍ خاصة.» وتُفتح النافذة من جديد.

بعد ذلك يمكن في هذا الحساب أيضًا تعطيل مربعات عرض / إدارة والإجراءات تحت **التفاصيل** واحدًا واحدًا.

ويعمل الزر حتى لو لم يكن في النظام إلا حساب واحد بدور المسؤول (Admin): فما دام هناك حساب Root مفعَّل يسمح الخادم بإزالة دور آخر حساب مسؤول وبتعطيل الحساب أو حذفه (وآخر Root مفعَّل محميّ على حدة). ولا يرفض الخادم تغيير دور آخر حساب مفعَّل بدور المسؤول (Admin) إلا إذا لم يوجد حساب Root مفعَّل: وعندئذ يبقى الحساب على دوره ولا يتغيّر وصوله كذلك. ويمكن تغيير الدور عبر REST API أيضًا (`PUT /auth/v1/users/{name}`، والمحتوى `{ "role": "Viewer" }`؛ لـ Root فقط).

أعمال خاصة بـ ROOT وحده

ما يلي لا يمكن منحه لأي مستخدم أو مجموعة؛ ينفّذه حساب Root فقط (ولا ينفّذه الإعداد المسبق «المدير» ولا الحساب القديم بدور المسؤول). ولا يرد في قائمة الإجراءات كذلك:

إدارة المستخدمين والمجموعات، **الوصول إلى الموارد (تقييد القنوات / الأجهزة)**، **إدارة أمان المساعد و MCP** (سطر المعلومات في نافذة الصلاحيات).

تبويبات **الاحتفاظ** و**الأمان** و**نسخ احتياطي** في الإعدادات؛ وقائمة النسخ الاحتياطية وسجل إصدارات التهيئة والرجوع إلى إصدار سابق؛ وتغيير خادم إرسال البريد الإلكتروني / SMS.

حذف سجل التدقيق وسجل الأحداث (زر **مسح السجل** في تبويب التدقيق وزر **مسح السجل** في سجل الأحداث).

تصدير المشروع الكامل واستيراده (**التصدير** / **استيراد** في صفحة الاتصال؛ ومن ضمنه استيراد Kepware JSON).

تفعيل الوصول المجهول في وكيل REST Server ضمن جسر البيانات.

الصلاحيات القديمة عند الترقية

عند الترقية إلى 3.10.1 لا يفقد أحد وصوله. مجموعات الصلاحيات المحفوظة الخاصة بالمستخدمين والمجموعات تُوسَّع مرة واحدة؛ ولا يكون لدى أحد قيد إجراءات (يبدأ الجميع بلا قيود):

إن كان في المجموعة القديمة	يُضاف

الاتصال: عرض (قراءة التهيئة)	العدّادات والمقاييس: عرض، إدارة المياه: عرض، التقارير: عرض، الأتمتة: عرض
الاتصال: إدارة (كتابة التهيئة)	العدّادات والمقاييس: إدارة، إدارة المياه: إدارة، التقارير: إدارة، الأتمتة: إدارة، جسر البيانات
الإنذارات	الإنذارات: إدارة (كان من يرى الإنذارات يستطيع تعديل تعريفاتها أيضًا)
سجلات البيانات	سجلات البيانات: إدارة

> **ضيّق الصلاحيات بعد الترقية** الترحيل سخيّ عن قصد، كي يبقى ما كان ممكنًا بالأمس ممكنًا اليوم. بعد الترقية راجع المجموعات والمستخدمين ذوي الصلاحيات الخاصة: أزل علامات «إدارة» غير اللازمة (مثل «الإنذارات: إدارة» لمشغّل يكفيه أن يتابع الإنذارات)، وعطّل عبر **التفاصيل** الإجراءات التي لا رجعة فيها مثل الحذف.

الصلاحية ليست هي الوصول إلى الموارد (ACL)

	الصلاحية والإجراء	الوصول إلى الموارد
السؤال	أي عمل يستطيع أداءه (إقرار إنذار، تصميم تقرير، حذف قناة)؟	على أي قنوات وأجهزة ومناطق وشاشات؟
أين	زر **الصلاحيات**	زر **الوصول** (في صف المستخدم أو المجموعة)؛ وفي النافذة قسما **الاتصال** و**SCADA**
الافتراضي	بلا مجموعة وبلا صلاحيات خاصة: صلاحيات الإعداد المسبق «مشاهد»	المستخدم غير Root لا يرى قناة أو جهازًا لم يُمنح الوصول إليه. مربع **كل الاتصالات (كل قناة + جهاز)** يفتح كل الاتصالات، ومربع **كل SCADA (كل المناطق والشاشات)** يفتح كل الشاشات.
الاتحاد	المستخدم ∪ المجموعة	المستخدم ∪ المجموعة (الوصول الآتي من المجموعة يظهر في النافذة بشارة «مجموعة»)

يُتحقَّق من الاثنين معًا: المستخدم الذي يملك «إدارة المياه: عرض» لا يرى في صفحات المياه إلا عدّادات الأجهزة التي يستطيع الوصول إليها. إن بدت الصفحة فارغة فانظر أولًا إلى زر **الوصول**. وطلب مثل «لا يرَ هذا المستخدم أجهزة ذلك الخط إطلاقًا» يُلبّى بالوصول إلى الموارد لا بالصلاحية.

> **تحذير** كلمة مرور المسؤول إلزامية عند التثبيت (لا يمكن تركها فارغة). تُضاف كلمة المرور المُدخلة في التثبيت الأول إلى حساب الويب `administrator` وكذلك كمستخدم OPC UA؛ والقائمتان منفصلتان: تغيير كلمة مرور الويب لاحقًا لا يغيّر كلمة مرور OPC UA. في الأنظمة المرقّاة من الإصدارات القديمة يبقى اسم الحساب `admin` ولا تُمسّ قائمة OPC UA. إذا أُدخلت كلمة مرور أثناء التثبيت فلا تُطلب مجددًا عند أول تسجيل دخول؛ أما الافتراضي `administrator/admin` فيُغيَّر عند أول تسجيل دخول فقط في قاعدة بيانات التطوير التي لم تُمسّ. قفل تسجيل الدخول: يُقفل بعد 8 محاولات خاطئة (HTTP 429). كلمة المرور القوية ضرورية في التثبيت المكشوف على الإنترنت.

انظر أيضًا مرجع الإجراءات · أمثلة من المصنع · الأسئلة الشائعة · الصلاحيات صفحةً بصفحة · كلمات المرور والجلسات · HTTPS / النشر العام · صلاحيات المساعد و REST API · MCP

مرجع الإجراءات: ما الذي تتيحه كل صلاحية وكل إجراء

الإصدار `3.10.1`

هذا القسم مرجع لكل صف في نافذة الصلاحيات ولكل مربع إجراء تحت **التفاصيل**: **31 صلاحية** و**95 إجراءً** في 16 وحدة. الأسماء كما تظهر في النافذة. والرمز تحت الاسم هو المفتاح المستخدم في REST API وفي استجابة 403 وفي سجل التدقيق: اسم الصلاحية على هيئة `AlarmsManage` ، ومفتاح الإجراء على هيئة `alarms.ack` .

كيف تُقرأ الجداول

الصف الغامق صلاحية (مربع «عرض» أو «إدارة» أو مربع منفرد في النافذة). إذا لم تُمنح الصلاحية لم تُرَ الوحدة أو لم تُدَر؛ ولا يُنظر في إجراءاتها أصلًا.

الصفوف تحته هي إجراءات تلك الصلاحية. عند منح الصلاحية تكون كلها مفعّلة؛ ثم تُعطَّل واحدًا واحدًا عبر **التفاصيل**. الإجراء المعطَّل لا يعمل زرّه ولا عنصره في قائمة النقر بالزر الأيمن ولا اختصاره في لوحة المفاتيح؛ والخادم يرفض العمل نفسه عبر REST والمساعد و MCP كذلك.

الصلاحية التي لا إجراءات لها (مثل: الاتصال: عرض، SCADA: عرض، الأتمتة: عرض، جدار الحماية، سجل التدقيق) تُمنح أو لا تُمنح فحسب.

في Root وفي الحساب القديم بدور المسؤول (Admin) لا يمكن تعطيل الإجراءات (في حساب Admin اضغط أولًا **إزالة الدور مع إبقاء الصلاحيات**؛ انظر الأدوار والصلاحيات).

قواعد عامة

النسخ يُعدّ إضافة (نسخ قناة = «إضافة قناة»)؛ و**الحذف الجماعي** يتطلب إجراء «الحذف».

إضافة **مجموعة وسوم** / تعديلها / حذفها و**توليد الوسوم** (دون اتصال، بالاتصال، جلب العُقد من الجهاز) من إجراءات الوسوم.

التقرير وصفحة التقرير وقائمة متابعة العدّادات أسرة إجراءات واحدة (إضافة / تعديل / حذف؛ بلا تمييز بحسب النوع).

ثلاثة إجراءات تصدير تُطبَّق في الواجهة فقط (سجل الإنذارات، بيانات العدّادات، تقارير المياه): يُنتَج الملف في المتصفح ويُخفى الزر؛ ومن يستطيع رؤية البيانات نفسها يستطيع قراءتها عبر REST. أما تصدير سجلات البيانات وتنزيل التقارير فيرفضهما الخادم أيضًا.

ما دام التعديل معطّلًا تُفتح النافذة للقراءة فقط: تُرى القيم، ولا يظهر **حفظ** (ولا «حذف»). أما الأدوات المساعدة مثل التحقق والمعاينة وقوائم الاختيار فتواصل العمل.

ما دامت إعادة التحميل معطّلة يحفظ المستخدم التعريف؛ لكن التغيير لا ينتقل إلى النظام العامل حتى يطبّقه مَن يملك صلاحية إعادة التحميل. ويُبلَّغ المستخدم بذلك مرة واحدة في الجلسة: «تم الحفظ. يلزم مستخدم يملك صلاحية إعادة التحميل لتطبيق التغيير على النظام العامل.»

رفض الخادم يُكتب في الواجهة باسم الإجراء: «ليست لديك صلاحية لهذا الإجراء: حذف تعريف الإنذار».

الاتصال

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
الاتصال: عرض `ConfigRead` صلاحية	يرى شجرة المشروع (القنوات والأجهزة والوسوم) وصفحتي الوسوم الافتراضية واختصارات الوسوم والقيم المباشرة وسجل الأحداث.	مثال: من دونها يسجّل المستخدم الدخول لكن شجرة المشروع تبقى فارغة؛ ومعظم الوحدات تتطلبها أيضًا.
الاتصال: إدارة `ConfigWrite` صلاحية	يضيف القنوات والأجهزة والوسوم والوسوم الافتراضية واختصارات الوسوم ويعدّلها ويحذفها. في التفاصيل يمكن تعطيل «إضافة / تعديل / حذف» لكل كائن على حدة.	مثال: يمكن إبقاء إضافة الوسوم وتعديلها مفعّلة لفني الصيانة مع تعطيل حذف القنوات والأجهزة.
إضافة قناة `channel.create`	يضيف قناة جديدة. نسخ القناة يُعدّ إضافة أيضًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل القناة `channel.edit`	يغيّر إعدادات قناة موجودة.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف القناة `channel.delete`	يحذف قناة. عند حذف قناة لا يُتحقَّق على حدة من «حذف الجهاز» / «حذف الوسم» للأجهزة والوسوم التي بداخلها.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
إضافة جهاز `device.create`	يضيف جهازًا جديدًا. نسخ الجهاز واستيراد الأجهزة من ملف يُعدّان إضافة أيضًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.

تعديل الجهاز `device.edit`	يغيّر إعدادات جهاز موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف الجهاز `device.delete`	يحذف جهازًا. عند حذف جهاز لا يُتحقَّق على حدة من «حذف الوسم» للوسوم التي بداخله.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
إضافة وسم `tag.create`	يضيف وسمًا جديدًا. يشمل ذلك مجموعات الوسوم وعمليات الوسوم الجماعية / CSV.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل الوسم `tag.edit`	يغيّر إعدادات وسم موجود. يشمل ذلك مجموعات الوسوم وعمليات الوسوم الجماعية / CSV.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف الوسم `tag.delete`	يحذف وسمًا. يشمل ذلك مجموعات الوسوم وعمليات الوسوم الجماعية / CSV.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
إضافة وسم افتراضي `vtag.create`	يضيف وسمًا افتراضيًا جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل وسم افتراضي `vtag.edit`	يغيّر إعدادات وسم افتراضي موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف الوسم الافتراضي `vtag.delete`	يحذف وسمًا افتراضيًا.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
إضافة اختصار وسم `alias.create`	يضيف اختصار وسم جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل اختصار الوسم `alias.edit`	يغيّر إعدادات اختصار وسم موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف اختصار الوسم `alias.delete`	يحذف اختصار وسم.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.

SCADA

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
SCADA: عرض `Scada` صلاحية	يفتح شاشات SCADA ويشغّلها.	مثال: بهذه الصلاحية وحدها يتابع المستخدم الشاشات؛ وإصدار الأوامر يتطلب أيضًا الكتابة إلى الوسوم.

SCADA: إدارة `ScadaDesign` صلاحية	يصمّم الشاشات: يضيفها ويعدّلها ويحذفها؛ ويدير المكتبة والرسوم الخلفية وشجرة المناطق.	مثال: يمكن إبقاء تعديل الشاشات مفعّلًا للمصمّم مع تعطيل حذف الشاشات.
إضافة شاشة `screen.create`	يضيف شاشة جديدة. تكرار الشاشة واستيرادها من ملف يُعدّان إضافة أيضًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل الشاشة `screen.edit`	يغيّر إعدادات شاشة موجودة. تعديل الشاشة في وضع التصميم وحفظها (إضافة كائنات، رسم) هو هذا الإجراء؛ وكذلك أدوات المساعد التي تغيّر الشاشة.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف الشاشة `screen.delete`	يحذف شاشة.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
مكتبة الرموز `scada.library`	يضيف كائناته ورموزه الخاصة إلى المكتبة ويعيد تسميتها ويحذفها.	عند التعطيل يستخدم المصمّم كائنات المكتبة لكنه لا يستطيع حفظ كائنات جديدة.
الرسوم الخلفية للشاشات `scada.art`	يرفع ملفات الرسوم الخلفية للشاشات إلى الخادم. تُرفع الرسوم الخلفية عند تثبيت حزمة من مكتبة الأجهزة.	عند التعطيل تُنشأ شاشات الحزمة المثبّتة من المكتبة لكن ملفات الرسوم الخلفية لا تُرفع؛ ويذكر تقرير التثبيت ذلك.
شجرة المناطق `scada.zones`	يضيف المناطق (شجرة المساحات / المنشأة) التي تجمع الشاشات ويعدّلها ويحذفها.	عند التعطيل لا يُفتح محرر المناطق؛ وتُضاف الشاشات إلى المناطق الموجودة.
مشاهدة الكاميرات `camera.view`	يشاهد الفيديو المباشر في مكوّن الكاميرا على شاشات SCADA ويلتقط لقطات. جزء من SCADA: عرض.	عند التعطيل تُفتح الشاشة ويظهر في مربع الكاميرا "ليس لديك إذن لمشاهدة الكاميرات"؛ ولا يخرج أي فيديو من الخادم.

الإنذارات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
الإنذارات: عرض `Alarms` صلاحية	يرى الإنذارات النشطة وسجل الإنذارات؛ ويقرّ الإنذارات ويصدّر السجل.	مثال: للوحة عرض للمتابعة فقط يمكن تعطيل الإقرار: يظهر الإنذار ولا يظهر زر «إقرار».
إقرار الإنذارات `alarms.ack`	يقرّ إنذارًا نشطًا.	عند التعطيل يرى المستخدم الإنذار لكن زر «إقرار» لا يظهر.
تصدير سجل الإنذارات `alarms.export`	ينزّل سجل الإنذارات كملف (CSV / Excel). يُطبَّق هذا القيد في الواجهة: يُنشأ الملف في المتصفح، لذلك لا يوجد منع مستقل في الخادم.	عند التعطيل يظهر السجل على الشاشة لكن زر التنزيل لا يظهر.
الإنذارات: إدارة `AlarmsManage` صلاحية	يضيف تعريفات الإنذارات ويعدّلها ويحذفها.	مثال: يمكن إبقاء تعديل التعريف (تغيير الحدود) مفعّلًا لمشغّل الوردية مع تعطيل الإضافة والحذف.
إضافة تعريف إنذار `alarmdef.create`	يضيف تعريف إنذار جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.

تعديل تعريف الإنذار `alarmdef.edit`	يغيّر إعدادات تعريف إنذار موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف تعريف الإنذار `alarmdef.delete`	يحذف تعريف إنذار.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.

سجلات البيانات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
سجلات البيانات: عرض `DataLogging` صلاحية	يستعلم عن السجل المحفوظ ويعرض مخططات الاتجاه ويصدّر البيانات.	مثال: مسؤول الجودة يرى السجل وينزّله لكنه لا يستطيع تعريف مجموعات التسجيل.
تصدير البيانات المسجّلة `log.export`	ينزّل السجل المحفوظ بصيغة CSV / Excel.	عند التعطيل يظهر المخطط والجدول لكن أزرار التنزيل لا تظهر.
سجلات البيانات: إدارة `DataLoggingManage` صلاحية	يضيف مجموعات التسجيل ويعدّلها ويحذفها؛ ويختار وجهة التسجيل؛ ويحذف البيانات القديمة.	مثال: عند تعطيل حذف البيانات القديمة يعرّف المستخدم المجموعات لكنه لا يستطيع حذف البيانات المسجّلة.
إضافة مجموعة تسجيل `loggroup.create`	يضيف مجموعة تسجيل جديدة.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل مجموعة التسجيل `loggroup.edit`	يغيّر إعدادات مجموعة تسجيل موجودة.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف مجموعة التسجيل `loggroup.delete`	يحذف مجموعة تسجيل.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
حذف البيانات القديمة `log.purge`	يحذف نهائيًا سجلات مجموعة التسجيل الأقدم من تاريخ معيّن.	عند التعطيل لا يظهر سطر «حذف البيانات القديمة».
وجهة التسجيل `loggroup.target`	ينشئ جدول مجموعة التسجيل في قاعدة البيانات الهدف، وينقل مجموعة قديمة إلى مصدر بيانات.	عند التعطيل لا يظهر زرّا «إنشاء الجدول» و«النقل إلى مصدر البيانات» في نافذة المجموعة.

العدّادات والمقاييس

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال

العدّادات والمقاييس: عرض `Metering` صلاحية	يرى قوائم العدّادات والمقاييس وحالتها وبيانات الفترات والأحداث؛ ويصدّر البيانات.	مثال: مسؤول الطاقة يتابع الاستهلاك وينقله إلى Excel.
تصدير بيانات العدّادات `metering.export`	ينزّل تقرير فترات العدّادات بصيغة Excel / CSV. يُطبَّق هذا القيد في الواجهة: يُنشأ الملف في المتصفح، لذلك لا يوجد منع مستقل في الخادم.	عند التعطيل تظهر الجداول لكن أزرار التنزيل لا تظهر.
العدّادات والمقاييس: إدارة `MeteringManage` صلاحية	يعرّف العدّادات والمقاييس ويُدخل القيم اليدوية ويجري التصحيحات ويدير الفئات والمجموعات.	مثال: عند إبقاء «إدخال القيم اليدوية» وحده مفعّلًا يُدخل المستخدم قيم الفواتير والتحاليل ولا يستطيع المساس بالتعريفات.
إضافة عدّاد `counter.create`	يضيف عدّادًا جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل العدّاد `counter.edit`	يغيّر إعدادات عدّاد موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف العدّاد `counter.delete`	يحذف عدّادًا.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
تصحيح العدّادات `counter.correct`	يجري تعديلًا يدويًا على عدّاد مقاس، ويسجّل استبدال العدّاد، ويضبط الإجمالي، ويبتّ في حالة التصفير.	عند التعطيل لا تظهر في نافذة العدّاد أزرار «التعديل اليدوي» و«استبدال العدّاد» و«ضبط الإجمالي» ولا زرّا قرار التصفير («العدّ من الصفر» و«اعتماده أساسًا جديدًا»).
إضافة مقياس `metric.create`	يضيف مقياسًا جديدًا. تعريفات المدخلات اليدوية تُعدّ مقاييس أيضًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل المقياس `metric.edit`	يغيّر إعدادات مقياس موجود. تعريفات المدخلات اليدوية تُعدّ مقاييس أيضًا.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف المقياس `metric.delete`	يحذف مقياسًا. تعريفات المدخلات اليدوية تُعدّ مقاييس أيضًا.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
إدخال القيم اليدوية `input.enter`	يكتب قيم الفترات في المدخلات اليدوية والعدّادات اليدوية (بما فيها إدخالات الهطول والتحاليل والإنتاج والموظفين والفواتير في صفحات المياه).	إذا أُبقي هذا وحده مفعّلًا يُدخل المستخدم قيم الفواتير والتحاليل الشهرية لكنه لا يستطيع تعريف العدّادات أو المقاييس.
الفئات والمجموعات `taxonomy.manage`	يضيف فئات العدّادات / المقاييس وشجرة المجموعات ويعيد تسميتها ويحذفها ويلوّنها. للمستخدمين الذين يصلون إلى كل الاتصالات؛ ولا يستطيع استخدامه من كان وصوله إلى الموارد مقيَّدًا.	عند التعطيل لا يظهر زر «الفئات والمجموعات».

إدارة المياه

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال

إدارة المياه: عرض `Water` صلاحية	يرى صفحات البصمة المائية وكفاءة المياه ومخطط تدفق المياه؛ ويصدّر التقارير. ويجب أن تكون مجموعة الميزات مفعّلة أيضًا.	مثال: المستخدم الذي لديه هذه الصلاحية وحدها يرى في القائمة صفحات إدارة المياه فقط.
تصدير تقارير المياه `water.export`	ينزّل جداول البصمة المائية وكفاءة المياه ومخطط تدفق المياه بصيغة Excel / CSV / PDF. يُطبَّق هذا القيد في الواجهة: يُنشأ الملف في المتصفح، لذلك لا يوجد منع مستقل في الخادم.	عند التعطيل تظهر الصفحات لكن أزرار التنزيل لا تظهر.
إدارة المياه: إدارة `WaterManage` صلاحية	يعرّف ملفات المياه والمخططات ويعدّلها ويحذفها؛ ويشغّل معالج الإعداد.	مثال: مسؤول المياه يعدّل الملفات؛ وتعريف العدّادات يتطلب أيضًا «العدّادات والمقاييس: إدارة».
إضافة ملف مياه `waterprofile.create`	يضيف ملف مياه جديدًا. ملفات البصمة المائية وكفاءة المياه ومخططات تدفق المياه.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل ملف المياه `waterprofile.edit`	يغيّر إعدادات ملف مياه موجود. ملفات البصمة المائية وكفاءة المياه ومخططات تدفق المياه.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف ملف المياه `waterprofile.delete`	يحذف ملف مياه. ملفات البصمة المائية وكفاءة المياه ومخططات تدفق المياه.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
معالج إعداد المياه `water.setup`	يسأل عن المصادر وأماكن الاستخدام ثم ينشئ العدّادات والمخطط والتقارير. يتطلب أيضًا «العدّادات والمقاييس: إدارة».	عند التعطيل لا يظهر زر «معالج الإعداد».

التقارير

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
التقارير: عرض `Reports` صلاحية	يفتح التقارير وصفحات التقارير وقوائم متابعة العدّادات ويشغّلها وينزّلها.	مثال: المدير يفتح التقرير وينزّل ملف PDF لكنه لا يستطيع تغيير تصميمه.
تنزيل التقارير `report.download`	ينزّل التقرير وصفحة التقرير وقائمة متابعة العدّادات بصيغة Excel / PDF / CSV. وما دام معطّلًا فإن مفاتيح الوصول إلى البيانات الخاصة بالمستخدم (قراءة الأنظمة الخارجية للتقارير) تتلقّى 403 كذلك.	عند التعطيل يُفتح التقرير على الشاشة لكن أزرار التنزيل لا تظهر.
التقارير: إدارة `ReportsManage` صلاحية	يصمّم التقارير وصفحات التقارير وقوائم متابعة العدّادات ويعدّلها ويحذفها.	مثال: يمكن إبقاء التصميم مفعّلًا لمختص التقارير مع تعطيل الحذف.
إضافة تقرير `report.create`	يضيف تقريرًا جديدًا. تقارير الجداول وصفحات التقارير وقوائم متابعة العدّادات؛ دون تمييز بحسب النوع.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل التقرير `report.edit`	يغيّر إعدادات تقرير موجود. تقارير الجداول وصفحات التقارير وقوائم متابعة العدّادات؛ دون تمييز بحسب النوع.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف التقرير `report.delete`	يحذف تقريرًا. تقارير الجداول وصفحات التقارير وقوائم متابعة العدّادات؛ دون تمييز بحسب النوع.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.

الأتمتة

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
الأتمتة: عرض `Workflows` صلاحية	يرى تدفقات الأتمتة وسجل التشغيل.	مثال: المشغّل يرى أي تدفق عمل ومتى، لكنه لا يستطيع تغيير التدفق.
الأتمتة: إدارة `WorkflowsManage` صلاحية	يعرّف التدفقات ويعدّلها ويحذفها ويفعّلها / يعطّلها.	مثال: يمكن إبقاء التفعيل / التعطيل مفعّلًا مع تعطيل التعديل: يوقف المستخدم التدفق لكنه لا يستطيع تغييره.
إضافة تدفق `workflow.create`	يضيف تدفقًا جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل التدفق `workflow.edit`	يغيّر إعدادات تدفق موجود.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف التدفق `workflow.delete`	يحذف تدفقًا.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
تفعيل التدفقات / تعطيلها `workflow.enable`	يفعّل التدفق أو يعطّله.	عند التعطيل لا يظهر مفتاح التفعيل / التعطيل في القائمة ولا في المحرر.

جسر البيانات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
جسر البيانات `DataBridge` صلاحية	يرى وكلاء جسر البيانات (MQTT و REST) ويضيفهم ويعدّلهم ويحذفهم ويختبرهم. صلاحية واحدة.	مثال: يمكن إبقاء تعديل الوكلاء مفعّلًا لمسؤول التكامل مع تعطيل الحذف.
إضافة وكيل `agent.create`	يضيف وكيلًا جديدًا.	عند التعطيل لا يظهر زر الإضافة؛ وتبقى العناصر الموجودة ظاهرة.
تعديل الوكيل `agent.edit`	يغيّر إعدادات وكيل موجود. المفاتيح العامة في تبويب جسر البيانات تُحفظ بهذا الإجراء أيضًا.	عند التعطيل تُفتح النافذة للقراءة فقط: لا يظهر زر «حفظ».
حذف الوكيل `agent.delete`	يحذف وكيلًا.	عند التعطيل لا يظهر زر «حذف» ولا خيار «حذف» في قائمة النقر بالزر الأيمن: يُمنع الحذف غير المقصود.
اختبار الوكلاء `agent.test`	يرسل طلبًا تجريبيًا إلى وجهة الوكيل، ويعاين وكيل التقارير.	عند التعطيل لا يظهر زر «طلب تجريبي» ولا أزرار المعاينة.

الكتابة إلى الوسوم والخدمات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال

الكتابة إلى الوسوم والخدمات `RuntimeControl` صلاحية	يكتب القيم إلى الوسوم، ويعيد تحميل وقت التشغيل، ويبدأ الخدمات / يوقفها، ويجري تشخيص الأجهزة، ويشغّل التدفقات يدويًا.	مثال: يُبقى لمشغّل الوردية «الكتابة إلى الوسوم» وحدها مفعّلة؛ ويُعطَّل إيقاف الخدمات.
الكتابة إلى الوسوم `tag.write`	يكتب قيمة إلى وسم من الواجهة أو من شاشة SCADA أو عبر REST (تشغيل مضخة، تحديد نقطة الضبط).	عند التعطيل لا تعمل أيقونة القلم في صفوف الوسوم ولا أزرار الأوامر في شاشات SCADA؛ وتبقى القيم ظاهرة.
إعادة تحميل وقت التشغيل `runtime.reload`	يطبّق تغيير الإعدادات على النظام العامل (يُعاد بناء المسح).	عند التعطيل يحفظ المستخدم التعريف، لكن التغيير لا يصل إلى النظام العامل حتى يطبّقه من يملك صلاحية إعادة التحميل.
بدء الخدمات / إيقافها `service.control`	يبدأ محرك المسح وخادم OPC UA ويوقفهما ويعيد تشغيلهما؛ ويفعّل إعادة التشغيل التلقائي ويعطّلها.	عند التعطيل لا تظهر أزرار «بدء / إيقاف / إعادة تشغيل» في الإعدادات › الخدمات.
تشخيص الجهاز `diag.run`	يراقب الحزم الخام المتبادلة مع الجهاز (نافذة التشخيص). أدوات تشخيص الشبكة لدى المساعد (ping و TCP و DNS والمنافذ المحلية) مرتبطة بهذا الإجراء أيضًا.	عند التعطيل لا يظهر «التشخيص» في صفحة الجهاز ولا في قائمة النقر بالزر الأيمن.
رفع الملفات `file.upload`	يرفع شهادة أو ملف ICD / SCL لإعداد قناة / جهاز.	عند التعطيل لا تظهر أزرار «استعراض» في نافذة الخصائص.
تشغيل التدفق يدويًا `workflow.run`	يبدأ تدفق أتمتة فورًا بزر «تشغيل». يتطلب أيضًا «الأتمتة: عرض».	عند التعطيل لا يظهر زر «تشغيل»؛ وتستمر التدفقات المجدولة والمُطلَقة بالوسوم في العمل.

عميل OPC UA

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
عميل OPC UA `OpcClient` صلاحية	يستخدم صفحة عميل OPC UA المدمج: يتصل ويتصفح ويشترك ويكتب.	مثال: مهندس التشغيل التجريبي يتصل بخادم بعيد ويتحقق من القيم؛ ويمكن تعطيل الكتابة إليه.
الاتصال والاكتشاف `uaclient.connect`	يتصل بخادم OPC UA بعيد ويقطع الاتصال به، ويكتشف الخوادم، ويفحص الشبكة.	عند التعطيل تظهر حالة الاتصال والاشتراكات لكن زر «اتصال» لا يظهر.
الكتابة إلى الخادم البعيد `uaclient.write`	يكتب قيمة إلى عقدة في خادم OPC UA المتصل.	عند التعطيل يمكن قراءة العقدة لكن زر «الكتابة» لا يظهر.
الاشتراكات `uaclient.subscribe`	يشترك في العقد ويزيل الاشتراكات.	عند التعطيل تُتابَع الاشتراكات الموجودة لكن لا يمكن إضافة اشتراكات جديدة.

القوالب والاستيراد

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
القوالب والاستيراد `Import` صلاحية	يثبّت القوالب ويحزّمها ويجري الاستيراد الجزئي. تصدير المشروع الكامل / استيراده لـ Root فقط.	مثال: يمكن إبقاء تثبيت القوالب مفعّلًا لمقاول خارجي مع تعطيل حذف القوالب.

تثبيت القوالب `template.install`	يثبّت قالبًا في المشروع (يضيف قنوات وأجهزة ووسومًا وشاشات). لا يُتحقَّق على حدة من إجراءات «الإضافة» للقنوات والأجهزة والوسوم والشاشات التي يثبّتها.	عند التعطيل تظهر القوالب لكن زر التثبيت في نافذة القالب لا يعمل.
تحزيم القوالب `template.package`	ينشئ قالبًا قابلًا لإعادة الاستخدام من جزء من المشروع؛ ويستورد قالبًا من ملف (.mhtpl). وتعديل قالب محفوظ هو هذا الإجراء أيضًا.	عند التعطيل لا يظهر زرّا «إنشاء قالب» و«استيراد (.mhtpl)».
حذف القوالب `template.delete`	يحذف قالبًا محفوظًا.	عند التعطيل لا يظهر زر «حذف» في نافذة القوالب.

الذكاء الاصطناعي و MCP

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
مساعد الذكاء الاصطناعي `Ai` صلاحية	يستخدم مساعد الذكاء الاصطناعي. كل أداة يشغّلها المساعد تتطلب أيضًا صلاحية ذلك العمل.	مثال: لا يستطيع المساعد أن ينفّذ نيابةً عن المستخدم ما لا يستطيع المستخدم نفسه تنفيذه.
MCP `Mcp` صلاحية	يستخدم صفحة MCP (الذكاء الاصطناعي): ينشئ رموز وصول لعميل ذكاء اصطناعي خارجي.	مثال: رمز الوصول لا ينفّذ إلا ما يُسمح به لصاحبه.
رموز وصول MCP `mcp.token`	ينشئ رموز الاتصال الشخصية لعميل ذكاء اصطناعي خارجي ويحذفها.	عند التعطيل تظهر صفحة MCP لكن لا يمكن إنشاء رموز وصول جديدة.
تنفيذ السكربتات `AiScripts` صلاحية	يستطيع المساعد تشغيل Python / PowerShell في البيئة المعزولة نيابةً عن هذا المستخدم. خطِر؛ ولا يُمنح إلا صراحةً.	مثال: يجب أيضًا أن يفعّل مدير النظام هذه الميزة؛ ويُطلب التأكيد عند كل تشغيل.
مزوّد الذكاء الاصطناعي `ai.provider` (ضمن صلاحية «إعدادات الخادم»)	يعرّف المزوّد وملف النموذج اللذين يستخدمهما المساعد ويختبرهما.	عند التعطيل لا يظهر تبويبا «المزوّدون» و MCP في إعدادات المساعد؛ يتحدث المستخدم مع المساعد لكنه لا يستطيع تعريف مزوّد أو مفتاح API.
مهارات المساعد `ai.skills` (ضمن صلاحية «إعدادات الخادم»)	يضيف مهارات المساعد ويعدّلها ويحذفها. أداة «حفظ المهارة» لدى المساعد مرتبطة بهذا الإجراء أيضًا.	عند التعطيل لا يظهر تبويب «المهارات» في إعدادات المساعد.
تعليمات إضافية `ai.prompt` (ضمن صلاحية «إعدادات الخادم»)	يكتب للمساعد تعليمات إضافية خاصة بالمنشأة.	عند التعطيل يكون حقل التعليمات الإضافية في إعدادات المساعد للقراءة فقط؛ ولا يمكن تغيير النص.

إعدادات الخادم والنظام

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
إعدادات الخادم `Settings` صلاحية	يدير إعدادات الخادم. في التفاصيل يمكن تعطيل كل قسم من الإعدادات على حدة.	مثال: يمكن أن يُترك لمسؤول الاتصال المؤسسي قسم «الهوية البصرية» وحده.

إعدادات خادم OPC UA `settings.opcua`	نقاط النهاية وسياسات الأمان ومستخدمو OPC UA.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
إعدادات الويب و REST API `settings.api`	عنوان الاستماع و HTTPS والوسطاء الموثوقون.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
إعدادات الوصول عبر الجوال `settings.mobile`	تسجيل الدخول من تطبيق الجوال والإشعارات الفورية وجلسات الأجهزة.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
إعدادات الهوية البصرية `settings.brand`	الشعار والاسم وشاشة تسجيل الدخول ومظهر البريد الإلكتروني. عنوان خلفية خريطة SCADA يُحفظ بهذا الإجراء أيضًا.	إذا أُبقي هذا وحده مفعّلًا يرى المستخدم في صفحة الإعدادات تبويب «الهوية البصرية» فقط.
مجموعات الميزات `settings.features`	يفعّل مجموعات الميزات في القائمة الجانبية (مثل إدارة المياه) ويعطّلها.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
الترخيص `settings.license`	يفعّل الترخيص ويحرّره، ويتحقق من التحديثات.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
مصادر البيانات `settings.datasources`	يدير اتصالات قواعد البيانات الخارجية ونسخ بيانات العدّادات إلى قاعدة بيانات خارجية (مخزن البيانات).	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
الخدمات وعتبات الموارد `settings.services`	يدير صفحة حالة الخدمات وعتبات تحذير الموارد وبدء تشغيل خدمة Windows. يشمل قسمَي إعدادات المراقبة (عتبات الموارد) والخدمة؛ أما بدء الخدمة / إيقافها فإجراء مستقل (بدء الخدمات / إيقافها).	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
مفاتيح الوصول إلى البيانات `settings.accesskeys`	ينشئ المفاتيح التي تتيح للأنظمة الخارجية قراءة التقارير ويحذفها.	عند التعطيل لا يمكن إنشاء مفاتيح في نافذة «القراءة من الأنظمة الخارجية» الخاصة بالتقرير.
إعدادات المسح `settings.scan`	يغيّر إعدادات محرك المسح.	ليس لهذا القسم تبويب في الواجهة؛ يُغيَّر الإعداد عبر REST أو MCP. عند التعطيل لا يستطيع المستخدم قراءة هذا القسم ولا تغييره.
إعدادات الكاميرا `settings.cameras`	يعرّف كاميرات IP (عنوان RTSP والمستخدم وكلمة المرور) ومحرك الفيديو.	عند التعطيل لا يظهر تبويب الإعدادات › الكاميرات؛ ويمكن مواصلة مشاهدة الكاميرات على الشاشات.
إدارة VPN `vpn.admin`	يشغّل MergenHub VPN ويوقفه؛ يضيف أجهزة المودم الميدانية ويعدّلها ويلغيها؛ وينشئ روابط إعداد صالحة لاستخدام واحد.	عند التعطيل تكون صفحة الإضافات › VPN للعرض فقط: تظهر الحالة وقائمة المواقع ولا يمكن تغيير أي شيء.
جدار الحماية `Firewall` صلاحية	يفتح المنافذ المطلوبة في جدار حماية Windows.	مثال: زر «فتح المنافذ» في الإعدادات › خادم OPC UA يظهر بهذه الصلاحية.

سجل التدقيق `Audit` صلاحية	يرى سجل التدقيق (من فعل ماذا ومتى). حذف السجلات لـ Root فقط.	مثال: مشرف الوردية يتابع من هنا مَن كتب أي قيمة.

إعدادات الإشعارات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
إعدادات الإشعارات `Notifications` صلاحية	يدير إعدادات البريد الإلكتروني و SMS ومركز الاتصالات (التفعيل / التعطيل، اسم المرسِل، المستلمون، التجربة، القوالب). خادم الإرسال يضبطه Root فقط.	مثال: عند إبقاء مركز الاتصالات وحده مفعّلًا يعدّل المستخدم قوالب الرسائل لكنه لا يستطيع المساس بإعدادات البريد الإلكتروني و SMS.
إعدادات البريد الإلكتروني `notify.email`	يفعّل إشعار البريد الإلكتروني / يعطّله، ويضبط اسم المرسِل والمستلمين، ويرسل بريدًا إلكترونيًا تجريبيًا. خادم الإرسال (العنوان، المنفذ، بيانات الاعتماد) يضبطه Root فقط.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
إعدادات SMS `notify.sms`	يفعّل إشعار SMS / يعطّله، ويضبط اسم المرسِل والمستلمين، ويرسل رسالة SMS تجريبية. اتصال المزوّد (العنوان، بيانات الاعتماد) يضبطه Root فقط.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
مركز الاتصالات `notify.comm`	يعدّل قوالب الرسائل، ويرسل دعوات المستخدمين والرسائل الجماعية.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
إعدادات Slack / Telegram `notify.chat`	يشغّل إشعارات المحادثة (Slack وTelegram وWhatsApp) أو يوقفها؛ ويضبط عنوان Webhook الخاص بـ Slack وبوت Telegram ومحادثاته، ومعرّف رقم هاتف WhatsApp ورمز الوصول والقالب والمستلمين، ويرسل رسالة تجريبية.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.

الشهادات

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
الشهادات `Certificates` صلاحية	يدير قائمة الثقة في OPC UA وشهادة الخادم وشهادة الويب.	مثال: مهندس التشغيل التجريبي يثق بشهادة عميل جديد؛ ويمكن تركـ شهادة الويب معطّلة.
شهادات العملاء `cert.trust`	يثق بشهادات عملاء OPC UA ويرفضها ويستوردها ويحذفها.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
شهادة الخادم `cert.instance`	يعرض شهادة خادم OPC UA نفسه.	عند التعطيل لا يظهر تبويب هذا القسم في صفحة الإعدادات؛ ولا يستطيع المستخدم رؤية هذه الإعدادات ولا تغييرها.
شهادة الويب `cert.web`	ينشئ شهادة HTTPS ويرفعها ويزيلها.	عند التعطيل لا تظهر أزرار شهادة الويب (إنشاء، رفع، إزالة) في تبويب الإعدادات › الويب وREST API والجوال.

ROOT فقط (صلاحيات لا يمكن منحها)

الصلاحية / الإجراء	ما يتيحه	ماذا يحدث عند تعطيله / مثال
إدارة المستخدمين والمجموعات `Users` صلاحية	يدير المستخدمين والمجموعات. لـ Root فقط.	مثال: لا يمكن منحها لمستخدم آخر أو لمجموعة.

الوصول إلى الموارد (تقييد القنوات / الأجهزة) `Acl` صلاحية	يحدد القنوات / الأجهزة التي يستطيع المستخدمون والمجموعات الوصول إليها. لـ Root فقط.	مثال: لا يمكن منحها لمستخدم آخر أو لمجموعة.
إدارة أمان المساعد و MCP `AiAdmin` صلاحية	يدير إعدادات أمان المساعد و MCP (البيئة المعزولة للسكربتات، وضع الموافقة، خوادم MCP الخارجية). لـ Root فقط.	مثال: لا يمكن منحها لمستخدم آخر أو لمجموعة.

انظر أيضًا الأدوار والصلاحيات · أمثلة من المصنع · الصلاحيات صفحةً بصفحة · أدوات المساعد و REST API · MCP

أمثلة من المصنع: أي المربعات لمن

الإصدار 3.10.1

في المصنع لكل قسم عمله ومسؤوليته. تبيّن الأمثلة التالية خطوة بخطوة، لمهام نموذجية، أي المربعات تُحدَّد في نافذة الصلاحيات، وأي الإجراءات تُعطَّل تحت **التفاصيل**، وكيف يُمنح الوصول إلى الموارد. أسماء الإجراءات كما تُكتب في النافذة؛ وكلها في مرجع الإجراءات. الأمثلة نقطة بداية: أضف مربعات وأزل أخرى بحسب منشأتك.

الخطوات المشتركة في كل مثال

أنشئ مجموعة. الإعدادات ← الوصول ← المستخدمون، ثم **إضافة مجموعة** في بطاقة **مجموعات المستخدمين**؛ واكتب **اسم المجموعة** (مثل: مشغّلو الورديات). تُفتح المجموعة الجديدة بمربعات الإعداد المسبق «مشاهد».

طبّق الإعداد المسبق وعدّل المربعات. اضغط زر الإعداد المسبق المذكور في المثال، ثم حدّد مربعات عرض / إدارة الواردة في المثال أو أزل علاماتها.

عطّل الإجراءات. اضغط **التفاصيل** في الصف المعنيّ وأزل علامات المربعات التي يقول المثال «عطّلها». ثم اقرأ ملخّص **يستطيع / لا يستطيع** في الأسفل واضغط **حفظ**.

أسند المستخدم إلى المجموعة. في بطاقة **المستخدمون** اختر المجموعة من عمود **المجموعة** للمستخدم. إن كانت للمستخدم صلاحيات خاصة (نقطة على زر الصلاحيات) فافتح نافذته وحدّد مربع **دون صلاحيات خاصة (تسري صلاحيات المجموعة)**؛ وإلا اتّحدت صلاحياته الخاصة مع المجموعة وقد يبقى الإجراء الذي عطّلته في المجموعة مفعّلًا لديه.

امنح الوصول إلى الموارد. زر **الوصول** في صف المجموعة: حدّد القنوات والأجهزة في قسم **الاتصال**، والمناطق والشاشات في قسم **SCADA**. وإن لم يلزم تقييد: **كل الاتصالات (كل قناة + جهاز)** و**كل SCADA (كل المناطق والشاشات)**.

> **لشخص واحد** يمكن ذلك من دون مجموعة: في نافذة **الصلاحيات** للمستخدم أزل علامة **دون صلاحيات خاصة (تسري صلاحيات المجموعة)** وامنح ذلك المستخدم المربعات نفسها. وإن كان شخص ثانٍ سيؤدّي العمل نفسه فتحويله إلى مجموعة أسهل (عبر **نسخ من مستخدم آخر / مجموعة أخرى...**).

1. مشغّل الوردية: يتابع ويقرّ الإنذارات ويكتب إلى الوسوم؛ ولا يمسّ التعريفات

الخطوة	ما يُفعل
الإعداد المسبق	**المشغّل**.
عرض / إدارة	كما يأتي بها الإعداد المسبق: «عرض» فقط في الاتصال و SCADA والإنذارات وسجلات البيانات والعدّادات والمقاييس وإدارة المياه والتقارير والأتمتة؛ وبلا أي «إدارة». العمليات والأدوات: أبقِ **الكتابة إلى الوسوم والخدمات** و**مساعد الذكاء الاصطناعي**؛ وأزل **عميل OPC UA** إن لم يلزم.
الإجراءات التي تُعطَّل	**الكتابة إلى الوسوم والخدمات** ‹ التفاصيل: أبقِ «الكتابة إلى الوسوم» وحده مفعّلًا؛ وأزل علامات «إعادة تحميل وقت التشغيل» و«بدء الخدمات / إيقافها» و«تشخيص الجهاز» و«رفع الملفات» و«تشغيل التدفق يدويًا». لا تمسّ صفّي الإنذارات والتقارير: يبقى «إقرار الإنذارات» و«تنزيل التقارير» مفعّلين.
الوصول إلى الموارد	قنوات وأجهزة الخط الذي تتولّاه الوردية؛ وفي قسم SCADA منطقة ذلك الخط.

النتيجة	يتابع الشاشات، ويعطي الأوامر بأزرار SCADA، ويقرّ الإنذارات، ويطّلع على السجل والمخطط. يفتح تعريف الإنذار للقراءة فقط؛ ولا يستطيع إضافة قناة أو جهاز أو وسم أو شاشة أو مجموعة تسجيل؛ ولا يستطيع إيقاف الخدمة.

2. مشرف الوردية: ما يفعله المشغّل + تغيير الحدود وإيقاف التدفقات والتدقيق

الخطوة	ما يُفعل
الإعداد المسبق	**المشغّل**، ثم المربعات التالية.
عرض / إدارة	**الإنذارات**: إدارة. **الأتمتة**: إدارة. و**سجل التدقيق** في قسم النظام.
الإجراءات التي تُعطَّل	**الإنذارات** › التفاصيل: في صف «تعريف الإنذار» أزل علامتَي **إضافة** و**حذف** وأبقِ **تعديل** (يغيّر الحدود، ولا يضيف تعريفًا ولا يحذفه). **الأتمتة** › التفاصيل: في صف «التدفق» أزل علامات **إضافة** و**تعديل** و**حذف** وأبقِ «تفعيل التدفقات / تعطيلها» (يوقف التدفق، ولا يغيّر محتواه). **الكتابة إلى الوسوم والخدمات** › التفاصيل: أبقِ «الكتابة إلى الوسوم» و«تشغيل التدفق يدويًا» و«تشخيص الجهاز»؛ وأزل علامتَي «بدء الخدمات / إيقافها» و«رفع الملفات».
الوصول إلى الموارد	كل الخطوط التي يتولّاها؛ وفي معظم المنشآت «كل الاتصالات» و«كل SCADA».
النتيجة	إضافةً إلى ما يفعله المشغّل: يغيّر حدّ الإنذار، ويوقف تدفقًا ويشغّله أو يشغّله يدويًا، ويتابع في تبويب **الإعدادات** ← **التدقيق** مَن كتب أي قيمة. والملخّص في قائمة المستخدمين يظهر على هيئة «الإنذارات: إدارة (إضافة تعريف إنذار, حذف تعريف الإنذار معطّل)».

3. فنّي الصيانة / الأتمتة: يضيف القنوات والأجهزة والوسوم ويعدّلها؛ ولا يحذف

الخطوة	ما يُفعل
الإعداد المسبق	**الصيانة**.
عرض / إدارة	الإعداد المسبق يدير كل الوحدات. أزل ما ليس من عمل الفنّي: إدارة المياه: إدارة، التقارير: إدارة، جسر البيانات، MCP، الشهادات، جدار الحماية.
الإجراءات التي تُعطَّل	**الاتصال** › التفاصيل: أزل علامات المربعات الخمسة في عمود **حذف** من الشبكة (القناة، الجهاز، الوسم، الوسم الافتراضي، اختصار الوسم). تظهر في الصف شارة «مقيَّدة: عدد الإجراءات المعطَّلة 5». وإن شئت فبالطريقة نفسها: **SCADA** › «الشاشة» **حذف**؛ **الإنذارات** › «تعريف الإنذار» **حذف**؛ **سجلات البيانات** › «مجموعة التسجيل» **حذف** و«حذف البيانات القديمة»؛ **القوالب والاستيراد** › «حذف القوالب». **الكتابة إلى الوسوم والخدمات** › أبقِ «إعادة تحميل وقت التشغيل» مفعّلًا (وإلا لم ينتقل الوسم الذي يضيفه إلى النظام العامل)؛ وأزل علامة «بدء الخدمات / إيقافها».
الوصول إلى الموارد	قنوات الخطوط التي يتولّاها. ويرى دائمًا القناة والشاشة اللتين أضافهما بنفسه.
النتيجة	يضيف القنوات والأجهزة والوسوم، ويغيّر خصائصها، ويجري تشخيص الجهاز، ويثبّت القوالب. زر الحذف وعنصر الحذف في قائمة النقر بالزر الأيمن ومفتاح Delete لا تعمل. عطّل مربعات الحذف الثلاثة معًا: فإذا بقي «حذف القناة» مفعّلًا أمكن حذف القناة مع ما بداخلها من أجهزة ووسوم.

4. مسؤول الطاقة / المياه: يتابع العدّادات وصفحات المياه ويُدخل القيم يدويًا؛ ولا يعرّف عدّادات

الخطوة	ما يُفعل
الإعداد المسبق	**مشاهد**، ثم المربعات التالية.
عرض / إدارة	**العدّادات والمقاييس**: إدارة. **إدارة المياه**: عرض (و«إدارة» إن كان سيعدّل الملفات والمخططات أيضًا). **التقارير**: عرض. وأزل SCADA والأتمتة إن لم يلزما.
الإجراءات التي تُعطَّل	**العدّادات والمقاييس** › التفاصيل: أبقِ «إدخال القيم اليدوية» وحده مفعّلًا. أزل علامات **إضافة** و**تعديل** و**حذف** في صف «العدّاد»؛ و**إضافة** و**تعديل** و**حذف** في صف «المقياس»؛ ومربعَي «تصحيح العدّادات» و«الفئات والمجموعات» (8 إجراءات). ويبقى «تصدير بيانات العدّادات» و«تنزيل التقارير» ضمن التقارير مفعّلين.
الوصول إلى الموارد	القنوات والأجهزة المرتبطة بها العدّادات (صفحات المياه لا تعرض إلا عدّادات الأجهزة المتاحة)؛ وإن كان للمنشأة كلها فـ«كل الاتصالات».

شرط مسبق	لصفحات المياه يجب أن تكون «إدارة المياه» مفعّلة في **الإعدادات** ← **مجموعات الميزات**.
النتيجة	يتابع الاستهلاك، وينقله إلى Excel، ويُدخل القيم الشهرية للفاتورة والتحليل والهطول والإنتاج (**إدخال قيمة الفترة** في العدّاد اليدوي). نوافذ العدّاد والمقياس تُفتح للقراءة فقط؛ ولا يظهر زرّا **التعديل اليدوي** و**استبدال العدّاد**. ومعالج إعداد المياه يتطلب «إدارة المياه: إدارة» و«العدّادات والمقاييس: إدارة» معًا.

5. الجودة / إعداد التقارير: يصمّم التقارير وينزّلها؛ ولا يرى إلا الأجهزة التي يعدّ تقاريرها

الخطوة	ما يُفعل
الإعداد المسبق	**مشاهد**، ثم المربعات التالية.
عرض / إدارة	**التقارير**: إدارة. **الاتصال**: عرض فقط (يختار الوسوم، ولا يضيف قنوات ولا أجهزة). وصلاحية «عرض» لكل مصدر بيانات سيستخدمه في التقارير: **الإنذارات** لسجل الإنذارات، **سجلات البيانات** للبيانات المسجّلة، **العدّادات والمقاييس** للعدّادات والمقاييس، **سجل التدقيق** لسجل التدقيق. المصدر الذي لا صلاحية له لا يُسرد في المحرّر.
الإجراءات التي تُعطَّل	**الإنذارات** › التفاصيل: أزل علامة مربع «إقرار الإنذارات» (يقرأ السجل ولا يقرّ الإنذارات). وإن شئت فأزل علامة مربع **حذف** في صف «التقرير» ضمن **التقارير** (يصمّم ولا يحذف).
الوصول إلى الموارد	طلب «ألّا يرى الأجهزة» يُلبّى هنا: في نافذة **الوصول** حدّد فقط القنوات والأجهزة التي سيعدّ تقاريرها. الجهاز غير المحدّد لا يظهر في شجرة المشروع ولا في منتقي الوسوم ولا في التقرير.
النتيجة	يصمّم التقارير وصفحات التقارير وقوائم متابعة العدّادات ويشغّلها وينزّلها بصيغ Excel / PDF / CSV. ولا يستطيع إضافة قناة أو جهاز أو وسم أو تعريف إنذار أو مجموعة تسجيل.

6. مصمّم SCADA: يصمّم الشاشات؛ ولا يعطي أوامر للميدان

الخطوة	ما يُفعل
الإعداد المسبق	**مشاهد**، ثم المربعات التالية.
عرض / إدارة	**SCADA**: إدارة. **الاتصال**: عرض (لربط الوسوم بالكائنات). لا تمنحه «الكتابة إلى الوسوم والخدمات»: فأزرار الأوامر في الشاشة لا تعمل لديه، والقيم تظهر.
الإجراءات التي تُعطَّل	عند الحاجة، **SCADA** › التفاصيل: **حذف** في صف «الشاشة» (يصمّم ولا يحذف)؛ و«شجرة المناطق» (يضيف الشاشات إلى المناطق الموجودة ولا يغيّر الشجرة). وأبقِ «مكتبة الرموز» مفعّلًا: يحفظ كائناته الخاصة في المكتبة.
الوصول إلى الموارد	في قسم الاتصال الأجهزة التي سيربطها بالشاشات؛ وفي قسم SCADA المناطق التي سيعدّلها. ويرى دائمًا الشاشة التي أنشأها بنفسه.
النتيجة	يضيف الشاشات ويعدّلها في وضع التصميم ويحفظها. نسخ شاشة أو استيرادها من ملف يُعدّ إضافة شاشة؛ أما تصدير المشروع الكامل / استيراده فلـ Root فقط.

7. مسؤول تقنية المعلومات / النظام: إعدادات الخادم تبويبًا تبويبًا

الخطوة	ما يُفعل
الحساب	في الحساب المُنشأ من الواجهة يمكن تعطيل الصلاحيات الممنوحة بالإعداد المسبق واحدةً واحدة. أما الحساب بدور المسؤول (Admin) القادم من إصدار أقدم أو المُنشأ عبر REST فلا يمكن تقييده: اضغط أولًا زر **إزالة الدور مع إبقاء الصلاحيات** في نافذة الصلاحيات.
الإعداد المسبق	**المدير** إن كان سيدير الميدان أيضًا؛ وإن كان سيُعنى بالخادم وحده فاضغط **مسح** في قسم **الوحدات** و**بلا** في قسم **العمليات والأدوات**، ثم المربعات التالية.
عرض / إدارة	في قسم النظام: **إعدادات الخادم**، **إعدادات الإشعارات**، **الشهادات**، **جدار الحماية**، **سجل التدقيق**. و**الكتابة إلى الوسوم والخدمات** إن كان سيبدأ الخدمات ويوقفها.

الإجراءات التي تُعطَّل	**إعدادات الخادم** › التفاصيل: كل مربع قسم إعدادات، وعند تعطيله لا يظهر ذلك التبويب. مثال: أبقِ «إعدادات خادم OPC UA» و«إعدادات الويب و REST API» و«إعدادات الوصول عبر الجوال» و«الترخيص» و«مصادر البيانات» و«الخدمات وعتبات الموارد»؛ وأزل علامات «إعدادات الهوية البصرية» و«مجموعات الميزات» و«مزوّد الذكاء الاصطناعي» و«مهارات المساعد» و«تعليمات إضافية» و«مفاتيح الوصول إلى البيانات». **إعدادات الإشعارات** › التفاصيل: «إعدادات البريد الإلكتروني» و«إعدادات SMS» و«مركز الاتصالات» كلٌّ على حدة. **الشهادات** › التفاصيل: «شهادات العملاء» و«شهادة الخادم» و«شهادة الويب». **الكتابة إلى الوسوم والخدمات** › التفاصيل: أبقِ «بدء الخدمات / إيقافها» وحده؛ وأزل علامات البقية ومنها «الكتابة إلى الوسوم».
الوصول إلى الموارد	إن لم يكن سيرى الميدان فلا تُحدَّد أي قناة.
النتيجة	لا يرى في صفحة الإعدادات إلا التبويبات التي أبقيتها مفعّلة (أي تبويب يرتبط بأي إجراء: الصلاحيات صفحةً بصفحة). أما تبويبات المستخدمون والاحتفاظ والأمان ونسخ احتياطي وخادم إرسال البريد الإلكتروني / SMS فتبقى Root J وحده.

8. المقاول الخارجي / المُكامِل: صلاحيات ضيّقة ومؤقتة

الخطوة	ما يُفعل
الحساب	أنشئ للمقاول حسابًا مستقلًا باسمه (**إضافة مستخدم**)؛ ولا تعطه حسابًا مشتركًا: فسجل التدقيق يكتب مَن فعل ماذا بحسب الحساب.
الإعداد المسبق	**مشاهد**، ثم المربعات التالية.
عرض / إدارة	**الاتصال**: إدارة. و**SCADA**: إدارة إن كان سيُنشئ شاشات أيضًا. العمليات والأدوات: **الكتابة إلى الوسوم والخدمات**، **عميل OPC UA** (لفحص الخادم البعيد أثناء التشغيل التجريبي)، **القوالب والاستيراد**. لا تمنحه شيئًا من قسم النظام؛ وإن لم تكن العدّادات والمياه والتقارير والأتمتة من عمله فأزل علامات مربعات «عرض» لها أيضًا.
الإجراءات التي تُعطَّل	**الاتصال** › التفاصيل: عمود **حذف** كله. **القوالب والاستيراد** › «حذف القوالب». **عميل OPC UA** › «الكتابة إلى الخادم البعيد». **الكتابة إلى الوسوم والخدمات** › «بدء الخدمات / إيقافها»؛ وأبقِ «الكتابة إلى الوسوم» و«إعادة تحميل وقت التشغيل» و«تشخيص الجهاز» و«رفع الملفات».
الوصول إلى الموارد	القنوات والمنطقة التي سيعمل عليها فقط. يرى القناة التي أضافها بنفسه؛ ولا يرى بقية المنشأة. وعند تثبيت قالب لا يستطيع الكتابة فوق مورد موجود لا يستطيع الوصول إليه.
المدة	ليس في الحساب حقل لتاريخ الانتهاء. عند انتهاء العمل أزل علامة مربع **مفعّل** للحساب في قائمة المستخدمين (يُعطَّل الحساب: لا يستطيع تسجيل الدخول، وتتوقف جلسته المفتوحة ورمز MCP الخاص به أيضًا) أو احذف الحساب. وفي العمل المتوقف مؤقتًا يكفي تحديد المربع من جديد.

9. مدير أعلى يكتفي بالمتابعة

الخطوة	ما يُفعل
الإعداد المسبق	**مشاهد**. المستخدم الجديد يُنشأ بهذه الصلاحيات أصلًا؛ ولا يلزم شيء خاص.
عرض / إدارة	**الإنذارات**: عرض إن كان سيرى حالة الإنذارات أيضًا؛ و**سجلات البيانات**: عرض لمخططات الاتجاه.
الإجراءات التي تُعطَّل	إن منحته «الإنذارات: عرض» فمن **الإنذارات** › التفاصيل: أزل علامة مربع «إقرار الإنذارات» (يرى الإنذار ولا يقرّه). وإن لم يُرَد التنزيل فمربع «تنزيل التقارير» ومربعات التصدير.
الوصول إلى الموارد	«كل الاتصالات» و«كل SCADA»؛ أو المنشأة التي يتولّاها فقط.
النتيجة	يرى الشاشات والعدّادات وصفحات المياه والتقارير، وينزّل التقرير. لا يستطيع تغيير أي شيء ولا الكتابة إلى الوسوم. ويتابع من الهاتف بالصلاحيات نفسها.

10. مستخدم العرض التجريبي / التعريفي

الخطوة	ما يُفعل
الإعداد المسبق	**مشاهد**.
عرض / إدارة	مربعات «عرض» للوحدات التي تريد عرضها (مثل: الإنذارات، سجلات البيانات). لا تمنحه أي «إدارة» ولا «الكتابة إلى الوسوم والخدمات» ولا أي مربع من قسم النظام.

الإجراءات التي تُعطَّل	إن لم يُرَد خروج البيانات: **التقارير** › «تنزيل التقارير»، **العدّادات والمقاييس** › «تصدير بيانات العدّادات»، **إدارة المياه** › «تصدير تقارير المياه»، **الإنذارات** › «إقرار الإنذارات» و«تصدير سجل الإنذارات»، **سجلات البيانات** › «تصدير البيانات المسجّلة».
الوصول إلى الموارد	القنوات والشاشات المعدّة للعرض التجريبي فقط؛ ولا تحدّد خطوط الإنتاج الحقيقية.
النتيجة	يتجوّل في الشاشات والصفحات التي اخترتها؛ ولا يستطيع تغيير أي شيء ولا تنزيله. وغيّر كلمة مرور حساب العرض المشترك بعد العرض (تُغلق الجلسات الأخرى).

11. مستخدم يرى إدارة المياه فقط

إضافة مجموعة؛ اضغط **مسح** في قسم **الوحدات**، ثم حدّد مربع «عرض» في صف **إدارة المياه** وحده.

اضغط **بلا** في قسمَي **العمليات والأدوات** و**النظام**. ثم **حفظ**.

أسند المستخدم إلى المجموعة؛ وامنحه عبر **الوصول** الأجهزة المرتبطة بها عدّادات المياه.

عند دخول المستخدم لا يرى تحت عنوان **الإضافات** في القائمة اليسرى إلا **إدارة المياه** والصفحات التي تحتها (إذا كانت «إدارة المياه» مفعّلة في **الإعدادات** ← **مجموعات الميزات**). لا تلزم صلاحية العدّادات: فأسماء الفئات والعدّادات تأتي مع الصفحة.

> **تحقّق** بعد الحفظ ادخل بحساب ذلك المستخدم (أو بحساب تجريبي في المجموعة نفسها) وافتح **ملفي الشخصي** › **صلاحياتي** › **ما الذي أستطيع فعله وما الذي لا أستطيعه؟**: يجب أن تطابق القائمة ما أعددته في النافذة.

انظر أيضًا الأدوار والصلاحيات · مرجع الإجراءات · الأسئلة الشائعة

الأسئلة الشائعة (الصلاحيات)

الإصدار `3.10.1`

لماذا لا أرى هذا الزر؟

انظر أولًا في حسابك إلى **ملفي الشخصي** › **صلاحياتي** › **ما الذي أستطيع فعله وما الذي لا أستطيعه؟**. لعدم ظهور الزر خمسة أسباب:

السبب	كيف يُعرف	من يصلحه
لا توجد صلاحية «إدارة» للوحدة	يُكتب في مربع «لا يستطيع»: «...: لا يدير (لا إضافة ولا تعديل ولا حذف)».	Root: مربع «إدارة» في نافذة الصلاحيات.
ذلك الإجراء معطَّل	يُكتب اسم الإجراء في مربع «لا يستطيع» (مثل: «الإنذارات: حذف تعريف الإنذار»)؛ ويظهر في ملخّص قائمة المستخدمين «(... معطّل)».	Root: زر **التفاصيل** في الصف. وإن كان المستخدم في مجموعة وجب أن يكون الإجراء مفعّلًا في المجموعة أيضًا.
لا وصول إلى المورد	ليس الزر هو الغائب، بل القناة أو الجهاز أو الشاشة نفسها؛ فتأتي الصفحة فارغة.	Root: زر **الوصول**.
مجموعة الميزات معطَّلة	صفحات إدارة المياه غير موجودة في القائمة.	مَن يملك صلاحية إعدادات الخادم: **الإعدادات** ← **مجموعات الميزات**.
العمل خاص بـ Root	تبويبات المستخدمون والاحتفاظ والأمان ونسخ احتياطي؛ تصدير المشروع الكامل / استيراده؛ حذف السجلات.	لا يُمنح؛ ينفّذه Root.

المستخدم يرى الشاشة لكنه لا يستطيع الحفظ

النافذة تُفتح للقراءة فقط ولا يوجد «حفظ». إجراء «التعديل» لذلك الكائن معطَّل (مثل: «تعديل الوسم»). وهذا هو السلوك المتوقع: تُرى القيم ولا يمكن تغييرها.

يحفظ لكن لا شيء يتغيّر في الميدان. إجراء «إعادة تحميل وقت التشغيل» معطَّل. يُقال للمستخدم مرة واحدة: «تم الحفظ. يلزم مستخدم يملك صلاحية إعادة التحميل لتطبيق التغيير على النظام العامل.» فإما أن يُفعَّل «إعادة تحميل وقت التشغيل» لذلك المستخدم ضمن **الكتابة إلى الوسوم والخدمات**، وإما أن يعيد التحميل مَن يملك الصلاحية.

رسالة «ليست لديك صلاحية لهذا الإجراء: ...». رفض الخادم الإجراء؛ والرسالة تذكر اسم الإجراء المعطَّل.

التعريف يشير إلى وسم لا يستطيع الوصول إليه. عند حفظ وسم افتراضي أو تدفق أو وكيل جسر بيانات أو مجموعة تسجيل يجب أن يكون كل وسم مُشار إليه متاحًا للمستخدم الذي يحفظ؛ والتعريف الذي يكتب إلى وسم يتطلب أيضًا «الكتابة إلى الوسوم والخدمات».

قسم في الإعدادات لا يُحفظ. إجراء ذلك القسم معطَّل (مثل: «إعدادات الهوية البصرية»)؛ وتبويبه لا يظهر أيضًا.

لماذا لا أستطيع تقييد المسؤول؟

الحساب الذي تحمل شارته **المسؤول** له في الخادم دور المسؤول (Admin): جاء من إصدار أقدم أو أُنشئ عبر REST. وهذا الدور كامل الصلاحيات دائمًا: لا تُطبَّق عليه إزالة علامات مربعات الصلاحيات ولا تعطيل الإجراءات؛ وفي نافذة الصلاحيات تكون مربعات الإجراءات مقفلة ويُكتب في القائمة «المسؤول: كامل الصلاحيات».

لتقييده اضغط زر **إزالة الدور مع إبقاء الصلاحيات** في نافذة صلاحيات الحساب ووافق: يُحوَّل الحساب إلى دور «مشاهد» وتُحفظ صلاحياته الحالية صلاحياتٍ خاصة؛ ولا يتغيّر وصوله. ثم عطّل الصلاحيات والإجراءات التي لا تريدها. ويعمل الزر حتى لو لم يكن في النظام إلا حساب واحد بدور المسؤول (Admin): فما دام هناك حساب Root مفعَّل يمكن إزالة دور آخر حساب مسؤول.

ولا حاجة إلى دور لمدير جديد: أنشئ المستخدم، وطبّق في نافذة الصلاحيات الإعداد المسبق **المدير** (أو أسند المستخدم إلى مجموعة)، ثم عطّل ما لا تريده.

كيف يُمنح قيد خاص لمستخدم في مجموعة؟

يكون الإجراء مفعّلًا إذا سمح به ملف المستخدم الخاص أو مجموعته. ولذلك لا تكفي إزالة علامة المربع لدى المستخدم لجعل شخص واحد في المجموعة **أضيق** صلاحيةً من المجموعة. هناك ثلاث طرق:

إن كان القيد يناسب الجميع فعطّل الإجراء في نافذة صلاحيات المجموعة: يُعطَّل لكل الأعضاء.

إن كان لشخص واحد فقط فأخرج ذلك المستخدم من المجموعة (**— (لا شيء)** في عمود **المجموعة**)، وانسخ صلاحيات المجموعة عبر **نسخ من مستخدم آخر / مجموعة أخرى...** في نافذة **الصلاحيات**، ثم عطّل الإجراء عبر **التفاصيل**.

إن كان لبضعة أشخاص فأنشئ مجموعة ثانية أضيق (انسخها وعطّل الإجراء) وانقل هؤلاء إليها.

وفي المقابل، منح شخص في المجموعة صلاحيات **أكثر** من المجموعة سهل: في نافذة المستخدم أزل علامة **دون صلاحيات خاصة (تسري صلاحيات المجموعة)** وحدّد المربع الإضافي؛ فتتّحد صلاحياته الخاصة مع مجموعته.

عطّلته لكنه ما زال يستطيع

ثلاثة احتمالات: مجموعة المستخدم تمنح الصلاحية نفسها بلا قيد (الملخّص في أسفل النافذة يعرض ذلك الإجراء مع «(من المجموعة)»)؛ أو الحساب بدور المسؤول (Admin) (السؤال أعلاه)؛ أو أن ما عطّلته أحد إجراءات التصدير الثلاثة (سجل الإنذارات، بيانات العدّادات، تقارير المياه) والمستخدم يقرأ البيانات عبر REST: فهذه الثلاثة تخفي الزر في الواجهة فقط، ولمنع رؤية البيانات أزل صلاحية «عرض».

هل تغيّرت الصلاحيات بعد الترقية؟

لم يفقد أحد وصوله. مجموعات الصلاحيات الخاصة المحفوظة ومجموعات صلاحيات المجموعات وُسِّعت مرة واحدة بصلاحيات عرض / إدارة الجديدة (الجدول: الأدوار والصلاحيات، «الصلاحيات القديمة عند الترقية»).

لا قيد إجراءات لدى أحد: الإجراءات الـ95 كلها تبدأ مفعّلة لكل من يملك الصلاحية الأم. والتضييق من عمل Root.

الحسابات التي لا مجموعة لها ولا صلاحيات خاصة نالت الافتراضي الجديد تلقائيًا.

ما ضاق: دور المسؤول (Admin) لا يستطيع قراءة أعداد الاحتفاظ ولا قائمتَي النسخ الاحتياطية والإصدارات، ولا حذف سجلات التدقيق والأحداث (لـ Root فقط)؛ وقراءة معلومات الإدارة صارت تتطلب صلاحية إدارتها. التفاصيل: «تغييرات السلوك» في ملاحظات الإصدار.

ما اتّسع: نافذة **الفئات والمجموعات** لم تعد لـ Root وحده (انظر الفئات والمجموعات).

الزر يظهر في الهاتف لكنه يقول «لا صلاحية»

تطبيق MergenHub Mobil لا يُظهر قيود الإجراءات على الأزرار بعد: إذا وُجدت صلاحية الوحدة ظهر الزر. وعند الضغط على إجراء معطَّل يرفض الخادم الطلب؛ وتأتي الرسالة بالإنجليزية (`Requires 'alarms.ack' permission.`). لا فرق من ناحية الأمان: القيد يُطبَّق في

الخادم. أما شاشة SCADA المفتوحة داخل التطبيق فهي واجهة الويب نفسها: وفيها يُطبَّق القيد على الزر أيضًا (مثلًا: إذا كان «الكتابة إلى الوسوم» معطّلًا فأزرار الأوامر لا تكتب).

هل تخضع API و MCP ومفاتيح الوصول للقاعدة نفسها؟

نعم. فحص الصلاحيات والإجراءات في الخادم؛ ولا فرق بين طرق الدخول.

الطريق	ما يحدث عند إجراء معطَّل
REST API (ملف تعريف الارتباط أو HTTP Basic)	403؛ وفي المحتوى مفتاح الإجراء: `{ "code": 403, "action": "alarms.ack", "message": "Requires 'alarms.ack' permission." }`
المساعد داخل التطبيق ورمز MCP الخارجي	الأداة التي عُطِّل إجراؤها لا تظهر في القائمة؛ وإن استُدعيت لم تعمل. ولا يتجاوز الرمز صلاحيات مالكه ولا قيوده.
مفتاح الوصول إلى البيانات (`mhkey_`)	إذا كان إجراء «تنزيل التقارير» معطّلًا لدى مالكه فالمفتاح لا يقرأ التقارير أيضًا (403).
تطبيق الجوال	يرفضه الخادم (السؤال أعلاه).
عملاء OPC UA	هذه الصلاحيات لواجهة الويب و REST API؛ أما مستخدمو OPC UA فقائمة مستقلة (الإعدادات ← مستخدمو OPC UA).

أين أرى مَن غيّر ماذا؟

الإعدادات ← التدقيق. تغييرات الصلاحيات والقيود تُكتب بتفاصيلها ضمن فئة «الأمان»: مَن، ولمن، الصلاحيات المضافة والمزالة، الإجراءات المعطَّلة والمفعَّلة. محاولة تنفيذ إجراء معطَّل لا تُسجَّل؛ وإنما يُسجَّل التغيير نفسه.

انظر أيضًا الأدوار والصلاحيات · مرجع الإجراءات · أمثلة من المصنع · REST API

الصلاحيات صفحةً بصفحة: أي زر يتطلب أي صلاحية وأي إجراء

الإصدار 3.10.1

يبيّن هذا القسم ما يقابل صفوف نافذة الصلاحيات في الصفحات. القاعدة العامة: **الصفحة التي لا تملك صلاحيتها لا تظهر في القائمة، والزر الذي لا تملك صلاحيته لا يُرسم في الصفحة**. أزرار عميل OPC UA و SCADA والإعدادات وجرس الإنذارات والمساعد في الشريط العلوي تظهر بحسب الصلاحيات أيضًا. إذا وصلت عبر رابط قديم إلى صفحة لا تملك صلاحيتها فُتحت صفحة المشروع. وإذا رُفض طلب مع ذلك ذكرت الرسالة اسم الصلاحية المطلوبة («يتطلب هذا الإجراء الصلاحيات التالية: العدّادات والمقاييس: إدارة، إدارة المياه: إدارة»).

الصلاحية هي باب الوحدة؛ ومعظم الأزرار في الصفحة مرتبط كذلك **بإجراء**، ويمكن تعطيل ذلك الإجراء عبر **التفاصيل** في نافذة الصلاحيات. في الجداول يُكتب اسم الإجراء كما في النافذة بين علاميَّ تنصيص وبجانبه مفتاحه. زر الإجراء المعطَّل لا يظهر؛ وإذا رُفض ذكرت الرسالة اسم الإجراء («ليست لديك صلاحية لهذا الإجراء: حذف تعريف الإنذار»). القائمة الكاملة: مرجع الإجراءات. وإذا لم يظهر زر فانظر أولًا إلى **ملفي الشخصي** › **صلاحياتي**.

المشروع والاتصال

العمل	المطلوب
إضافة القنوات والأجهزة والوسوم والوسوم الافتراضية واختصارات الوسوم وتعديلها وحذفها	**الاتصال: إدارة**. لكل كائن إجراءات مستقلة للإضافة والتعديل والحذف (`channel.create` … `alias.delete` ، 15 إجراءً). النسخ يُعدّ إضافة؛ ومجموعات الوسوم وتوليد الوسوم من إجراءات الوسوم؛ وما دام التعديل معطّلًا تُفتح نافذة الخصائص للقراءة فقط. وانتقال ما حُفظ إلى النظام العامل يتطلب إجراء «إعادة تحميل وقت التشغيل» (`runtime.reload`).
كتابة قيمة إلى وسم، فرض القراءة من الجهاز، تشخيص الجهاز، بدء خدمة / إيقافها	**الكتابة إلى الوسوم والخدمات**. الإجراءات: «الكتابة إلى الوسوم» (`tag.write`)؛ القلم في صف الوسم وأزرار الأوامر في SCADA)، «تشخيص الجهاز» (`diag.run`)، «بدء الخدمات / إيقافها» (`service.control`)، «إعادة تحميل وقت التشغيل» (`runtime.reload`)، «رفع الملفات» (`file.upload`)؛ زر «استعراض» في نافذة الخصائص). وليس لفرض القراءة من الجهاز إجراء مستقل.

زرّا **التصدير** و**استيراد** (المشروع الكامل؛ ومنه Kepware JSON)، والتصدير / الاستيراد في شريط أدوات تصميم SCADA	Root فقط. لا تظهر الأزرار في أي حساب آخر.
نافذة القوالب: **إنشاء قالب**، **استيراد (.mhtpl)**، التثبيت و**حذف**	**القوالب والاستيراد**. الإجراءات: «تثبيت القوالب» (`template.install`)، «تحزيم القوالب» (`template.package` ؛ ومنه استيراد ملف قالب)، «حذف القوالب» (`template.delete`). تلتزم بالوصول إلى الموارد: لا تحرّم إلا القنوات والشاشات التي تستطيع الوصول إليها؛ ولا يستطيع القالب الكتابة فوق مورد موجود لا تستطيع الوصول إليه. أما التصفح و**تصدير ملف** فيعملان بصلاحية «الاتصال: عرض».
حفظ وسم افتراضي	يجب أن يكون كل وسم يشير إليه التعبير متاحًا لك. إذا كان حقل **الخرج** مملوءًا (وسم افتراضي يكتب إلى وسم) لزمت أيضًا صلاحية «الكتابة إلى الوسوم والخدمات».
نافذة الاشتراكات والعملاء المتصلين التي تُفتح بالنقر على مؤشر الوسوم النشطة / العملاء في شريط الحالة	**إعدادات الخادم** أو **الكتابة إلى الوسوم والخدمات**

الإنذارات وسجلات البيانات

العمل	المطلوب
رؤية الإنذارات النشطة وإقرارها والسجل	**الإنذارات: عرض**. الإقرار هو إجراء «إقرار الإنذارات» (`alarms.ack`): إذا عُطِّل ظهر الإنذار ولم يظهر زر «إقرار». ونقل السجل إلى ملف هو إجراء «تصدير سجل الإنذارات» (`alarms.export`).
الإضافة والتعديل والحذف في تبويب **التعريفات**	**الإنذارات: إدارة**. الإجراءات: «إضافة تعريف إنذار»، «تعديل تعريف الإنذار»، «حذف تعريف الإنذار» (`alarmdef.create` ، `alarmdef.edit` ، `alarmdef.delete`). المستخدم الذي يملك «عرض» فقط أو عُطِّل له التعديل يفتح التعريف للقراءة فقط.
المخطط والاستعلام عن السجل والتصدير	**سجلات البيانات: عرض**. أزرار التنزيل مرتبطة بإجراء «تصدير البيانات المسجّلة» (`log.export`).
إضافة مجموعة تسجيل وتعديلها وحذفها؛ حذف البيانات القديمة؛ إضافة وسم إلى التسجيل من SCADA	**سجلات البيانات: إدارة**. الإجراءات: «إضافة مجموعة تسجيل»، «تعديل مجموعة التسجيل»، «حذف مجموعة التسجيل» (`loggroup.create` ، `loggroup.edit` ، `loggroup.delete`)، «حذف البيانات القديمة» (`log.purge`)، «وجهة التسجيل» (`loggroup.target` : إنشاء الجدول، النقل إلى مصدر بيانات). يجب أن يكون كل وسم يُضاف إلى المجموعة متاحًا لك.
اختبار الاتصال في نافذة مجموعة التسجيل	تكفي «سجلات البيانات: إدارة» لاختيار مصدر بيانات محفوظ واختباره؛ أما إدخال اتصال يدويًا واختباره فيتطلب **إعدادات الخادم**.

العدّادات والمقاييس، إدارة المياه، التقارير

العمل	المطلوب
تعريف العدّادات والمقاييس والمدخلات اليدوية؛ القيم اليدوية والتصحيح؛ **الفئات والمجموعات**	**العدّادات والمقاييس: إدارة**. الإجراءات: «إضافة عدّاد»، «تعديل العدّاد»، «حذف العدّاد» (`counter.create` ...)، «إضافة مقياس»، «تعديل المقياس»، «حذف المقياس» (`metric.create` ...؛ وتعريف المدخل اليدوي يُعدّ مقياسًا)، «إدخال القيم اليدوية» (`input.enter` : **إدخال قيمة الفترة**)، «تصحيح العدّادات» (`counter.correct` : **التعديل اليدوي**، **استبدال العدّاد**)، «الفئات والمجموعات» (`taxonomy.manage` ؛ ويتطلب أيضًا الوصول إلى كل الاتصالات). أما أزرار التصدير فهي إجراء «تصدير بيانات العدّادات» ضمن صلاحية «عرض» (`metering.export`).
تجربة في تفاصيل المقياس	العدّادات والمقاييس: إدارة. المستخدم الذي يملك «عرض» فقط يستطيع فتح تفصيل الفترة.
زر **مخزن البيانات** في صفحة العدّادات	**إعدادات الخادم** وإجراء «مصادر البيانات» (`settings.datasources`)
رؤية صفحات البصمة المائية وكفاءة المياه ومخطط تدفق المياه	**إدارة المياه: عرض** (لا تلزم صلاحية العدّادات؛ فأسماء الفئات والعدّادات تأتي مع الصفحة).

إعدادات ملف المياه والمخطط	**إدارة المياه: إدارة**. الإجراءات: «إضافة ملف مياه»، «تعديل ملف المياه»، «حذف ملف المياه» (`waterprofile.create` ، `waterprofile.edit` ، `waterprofile.delete`). أما زرّا التصدير والطباعة فهما إجراء «تصدير تقارير المياه» ضمن صلاحية «عرض» (`water.export`).
إدخال قيمة عدّاد يدوية أو هطول أو تحليل أو إنتاج أو عدد عاملين أو مساحة في الجدول ضمن صفحات المياه	**العدّادات والمقاييس: إدارة** وإجراء «إدخال القيم اليدوية» (`input.enter`). إذا كان معطّلًا لم يمكن النقر على خلايا القيم.
معالج إعداد المياه	إدارة المياه: إدارة والعدّادات والمقاييس: إدارة معًا؛ وكذلك إجراء «معالج إعداد المياه» (`water.setup`). إذا نقصت إحدى الصلاحيتين ذكر المعالج أيّهما الناقصة.
فتح تقرير أو صفحة تقرير أو قائمة متابعة عدّادات وتشغيلها وتنزيلها؛ وتحديث البطاقات المباشرة	**التقارير: عرض**. أزرار CSV / PDF / Excel هي إجراء «تنزيل التقارير» (`report.download`): إذا كان معطّلًا فُتح التقرير على الشاشة ولم يمكن تنزيله؛ ولا يعمل كذلك قالب Excel لقائمة متابعة العدّادات ولا مفاتيح الوصول إلى البيانات الخاصة بالمستخدم. والتقرير المبني على الإنذارات أو البيانات المسجّلة أو سجل التدقيق يتطلب أيضًا صلاحية «عرض» لذلك المصدر.
تصميم تقرير، معاينة تقرير غير محفوظ، الحذف	**التقارير: إدارة**. الإجراءات: «إضافة تقرير»، «تعديل التقرير»، «حذف التقرير» (`report.create` ، `report.edit` ، `report.delete`)؛ وهي واحدة للتقرير الجدولي وصفحة التقرير وقائمة متابعة العدّادات. اختيار مصدر في المحرّر يتطلب صلاحية «عرض» لذلك المصدر. وإنشاء مفتاح في نافذة «القراءة من الأنظمة الخارجية» في التقرير يتطلب صلاحية «إعدادات الخادم» وإجراء «مفاتيح الوصول إلى البيانات» (`settings.accesskeys`).
تبويب **تقارير Excel** في صفحة العدّادات والمقاييس	يظهر بصلاحية «التقارير: عرض»؛ والتصميم يتطلب «التقارير: إدارة». تغيير لون المجموعة يتطلب «العدّادات والمقاييس: إدارة».

الأتمتة

العمل	المطلوب
قائمة التدفقات وسجل التشغيل	**الأتمتة: عرض**. يُفتح التدفق للقراءة فقط؛ ولا يوجد زر **تحقق** ولا فحص للتعبير ولا ملخّص cron.
إضافة تدفق وتعديله وحذفه وتفعيله وتعطيله	**الأتمتة: إدارة**. الإجراءات: «إضافة تدفق»، «تعديل التدفق»، «حذف التدفق» (`workflow.create` ، `workflow.edit` ، `workflow.delete`) و«تفعيل التدفقات / تعطيلها» (`workflow.enable`). إذا كان التعديل معطّلًا والتفعيل / التعطيل مفعّلًا أوقف المستخدم التدفق لكنه لا يغيّر محتواه.
زر **تشغيل**	الأتمتة: عرض + **الكتابة إلى الوسوم والخدمات**؛ الإجراء: «تشغيل التدفق يدويًا» (`workflow.run`). وما دام معطّلًا تواصل التدفقات المجدولة والمشغَّلة بالوسوم عملها.
حفظ تدفق يكتب إلى وسم	الأتمتة: إدارة + الكتابة إلى الوسوم والخدمات؛ ويجب أن يكون كل وسم يُكتب إليه أو يُقرأ متاحًا لك.
حفظ تدفق يقرّ الإنذارات	إضافةً إلى ذلك صلاحية الإنذارات والوصول إلى وسم الإنذار.
تدفق يرسل بريدًا / SMS إلى مستلم ليس عنوان مستخدم مسجَّل ولا مستلم إشعارات إنذار	إضافةً إلى ذلك **إعدادات الإشعارات**.
تدفق يرسل طلب HTTP إلى الخادم نفسه (`localhost` و `127.x` و `169.254.x`)	إضافةً إلى ذلك **إعدادات الخادم**.

التدفق للقراءة فقط. التدفق الذي يشير إلى وسم لا تستطيع الوصول إليه، أو يحتوي على خطوة لا يحق لك تنفيذها، يظهر في القائمة مع **أيقونة قفل**. في المحرّر تُكتب شارة **للقراءة فقط** والسبب؛ ولا يوجد حفظ ولا حذف ولا تفعيل / تعطيل ولا تشغيل؛ وتأتي مسارات الوسوم ومفتاح Webhook وترويسات HTTP والمستلمون مقنّعة. تُطبَّق هذه القواعد **وقت الحفظ** فقط: التدفقات المحفوظة تواصل العمل.

مفتاح Webhook. في مشغِّل Webhook حقل **المفتاح** للقراءة فقط: يولّد الخادم المفتاح (32 حرفًا عشوائيًا) ولا يمكن كتابته يدويًا. زر **تجديد** يُفرغ المفتاح؛ فيُولَّد مفتاح جديد عند الحفظ ويتوقف العنوان القديم عن العمل. تعطي النظام الخارجي العنوان الموجود في حقل **نقطة النهاية**. يظهر تحذير للمفتاح القديم القصير (يستمر في العمل؛ استبدله عبر «تجديد»). نقطة النهاية `/hooks/` تقبل **60** طلبًا في الدقيقة على الأكثر من عنوان IP نفسه؛ وما زاد يعيد 429. لا يُحفظ محتوى استجابة خطوة HTTP في سجل التشغيل (يبقى رمز الحالة والمدة وعدد البايتات).

جسر البيانات

رؤية تبويب جسر البيانات وإدارة الوكلاء تتطلبان صلاحية **جسر البيانات**. الإجراءات: «إضافة وكيل»، «تعديل الوكيل»، «حذف الوكيل» (`agent.create` ، `agent.edit` ، `agent.delete`) و«اختبار الوكلاء» (`agent.test`) : **إرسال طلب اختبار** ومعاينة وكيل التقارير). والمفاتيح العامة في التبويب تُحفظ بإجراء «تعديل الوكيل». يجب أن يكون كل وسم يرسله الوكيل أو يتيح قراءته متاحًا للمستخدم الذي يحفظه.

الحقل	القاعدة
وكيل REST Server، **السماح بالوصول المجهول**	يبدأ غير محدّد في الوكيل الجديد؛ ولا يستطيع تفعيله إلا **Root**. وما دام معطّلًا تطلب نقطة النهاية `/iotgateway/` بيانات الدخول: يحتاج حساب القراءة إلى «الاتصال: عرض» والوصول إلى الوسوم التي يقرؤها، ويحتاج حساب الكتابة إلى «الكتابة إلى الوسوم والخدمات». الوسم الذي لا يراه الحساب لا يظهر في القائمة.
وكيل REST Server، **السماح بالكتابة**؛ وكيل MQTT، **موضوع الكتابة**	مقفلان إن لم تكن لديك صلاحية «الكتابة إلى الوسوم والخدمات». كل كتابة تُجرى عبر نقطة النهاية هذه تُسجَّل في سجل التدقيق.
تغيير الهدف (الخادم، المنفذ، المستخدم)	لا تُرسَل كلمة المرور / المفتاح المحفوظ إلى الهدف الجديد: يُدخل من جديد. زر **إرسال طلب اختبار** يتحقق من شهادة الهدف.

الإعدادات: كلٌّ يرى التبويبات التي يستطيع تغييرها فقط

التبويب	الصلاحية المطلوبة	الإجراء (عند تعطيله لا يظهر التبويب)
خادم OPC UA، مستخدمو OPC UA	**إعدادات الخادم**	«إعدادات خادم OPC UA» (`settings.opcua`)
الويب وREST API والجوال	إعدادات الخادم	«إعدادات الويب و REST API» (`settings.api`)
مصادر البيانات	إعدادات الخادم	«مصادر البيانات» (`settings.datasources`)
دفع الجوال	إعدادات الخادم	«إعدادات الوصول عبر الجوال» (`settings.mobile`)
الهوية البصرية	إعدادات الخادم	«إعدادات الهوية البصرية» (`settings.brand`)
مجموعات الميزات	إعدادات الخادم	«مجموعات الميزات» (`settings.features`)
الترخيص	إعدادات الخادم	«الترخيص» (`settings.license`)
الخدمات	إعدادات الخادم	«الخدمات وعتبات الموارد» (`settings.services`). أما أزرار بدء / إيقاف / إعادة تشغيل في الصفحة فتتطلب أيضًا إجراء «بدء الخدمات / إيقافها» ضمن صلاحية «الكتابة إلى الوسوم والخدمات».
العملاء الموثوقون	**الشهادات**	«شهادات العملاء» (`cert.trust`)
شهادة الخادم	الشهادات	«شهادة الخادم» (`cert.instance`)
أزرار شهادة الويب في تبويب الويب وREST API والجوال	الشهادات	«شهادة الويب» (`cert.web`)؛ إذا كان معطّلًا لم تظهر الأزرار
البريد الإلكتروني، SMS، الاتصالات	**إعدادات الإشعارات** (تغيير خادم إرسال البريد / SMS J Root فقط)	«إعدادات البريد الإلكتروني» (`notify.email`)، «إعدادات SMS» (`notify.sms`)، «مركز الاتصالات» (`notify.comm`)
جسر البيانات	**جسر البيانات**	يظهر التبويب بالصلاحية؛ والأزرار مرتبطة بإجراءات الوكلاء
التدقيق	**سجل التدقيق**	لا إجراءات لها
المستخدمون، الاحتفاظ، الأمان، نسخ احتياطي	Root فقط	لا يُمنح

ضمن صلاحية «إعدادات الخادم» إجراءان آخران لا تبويب لهما في الواجهة: «إعدادات المسح» (`settings.scan` ؛ يُغيَّر عبر REST أو MCP) و«مفاتيح الوصول إلى البيانات» (`settings.accesskeys` ؛ من نافذة التقرير). وإعدادات المساعد تتبع الصلاحية نفسها أيضًا:

تبويبا المزوّدون و MCP مرتبطان بإجراء «مزوّد الذكاء الاصطناعي» (`ai.provider`)، وتبويب المهارات بإجراء «مهارات المساعد» (`ai.skills`)، وحقل التعليمات الإضافية بإجراء «تعليمات إضافية» (`ai.prompt`).

المستخدم الذي لا يملك صلاحية أي تبويب لا يرى زر **الإعدادات**. بصمة الترخيص ومالكه ومعلومات التفعيل والإصدار الجديد لا تُعرض إلا لمستخدم يملك صلاحية «إعدادات الخادم»؛ وشارة الترخيص وكبسولة الوضع التجريبي لا يمكن النقر عليهما إلا له. في نافذة مجموعة التسجيل تكفي «سجلات البيانات: إدارة» **لاختيار** مصدر بيانات؛ أما إضافة المصدر وتعديله فتتطلبان «إعدادات الخادم».

عميل OPC UA و MCP

العمل	المطلوب
الاتصال وقطع الاتصال والبحث عن الخوادم في صفحة عميل OPC UA	**عميل OPC UA**؛ الإجراء: «الاتصال والاكتشاف» (`uaclient.connect`)
الاشتراك في عقدة وإزالة الاشتراك	عميل OPC UA؛ الإجراء: «الاشتراكات» (`uaclient.subscribe`)
كتابة قيمة إلى عقدة في الخادم البعيد	عميل OPC UA؛ الإجراء: «الكتابة إلى الخادم البعيد» (`uaclient.write`)
إنشاء الرموز وتعطيلها وحذفها في صفحة MCP (الذكاء الاصطناعي)	**MCP**؛ الإجراء: «رموز وصول MCP» (`mcp.token`)

سجل التدقيق وسجل الأحداث

تبويب **الإعدادات** ← **التدقيق** يظهر بصلاحية «سجل التدقيق». إضافةً إلى تغييرات التهيئة يُسجَّل ما يلي: **الكتابة إلى الوسوم** (الوسم = القيمة)، بدء خدمة / إيقافها / إعادة تشغيلها، تشغيل تدفق يدويًا، الكتابة عبر نقطة نهاية الكتابة في وكيل REST Server (مَن أو «مجهول»، وعنوان العميل)، واستدعاءات Webhook (المفتاح مقنّع). وتغييرات الصلاحيات وقيود الإجراءات تُكتب بتفاصيلها أيضًا (مَن، ولمن، الصلاحيات المضافة / المزالة، الإجراءات المعطَّلة / المفعَّلة). زر **مسح السجل** في تبويب التدقيق وزر **مسح السجل** في سجل الأحداث لا يظهران إلا لـ Root.

ماكروات SCADA

استعلامات `MH.query` في الماكرو تعمل بصلاحيات المستخدم الذي يفتح الشاشة: `alarms` و `alarmDefs` و `alarmHistory` تتطلب «الإنذارات: عرض»؛ و `audit` «سجل التدقيق»؛ و `subsystems` «إعدادات الخادم»؛ و `agents` «جسر البيانات»؛ و `loggerStatus` و `loggerGroups` «سجلات البيانات: عرض»؛ و `opcuaClients` «إعدادات الخادم» أو «الكتابة إلى الوسوم والخدمات». من دون الصلاحية يعيد الاستعلام رسالة «لا تملك صلاحية لهذه البيانات» بدل البيانات ولا يذهب أي طلب إلى الخادم.

انظر أيضًا الأدوار والصلاحيات · مرجع الإجراءات · أمثلة من المصنع · المساعد و MCP · جسر البيانات

كلمات المرور و«نسيت كلمة المرور» والجلسات

الإصدار `3.10.1`

نسيت كلمة المرور

في شاشة تسجيل الدخول انقر **نسيت كلمة المرور؟**؛ اكتب اسم المستخدم أو البريد الإلكتروني أو الهاتف واضغط **إرسال الرمز**.

يصل رمز تحقق من **8 أرقام** إلى البريد الإلكتروني أو الهاتف المسجَّل في حسابك. الرمز صالح لمدة **5 دقائق**.

اكتب الرمز كاملًا في حقل **رمز التحقق** وكلمة مرورك الجديدة تحته، ثم اضغط **إعادة تعيين كلمة المرور**. الرمز الناقص الأرقام لا يُرسَل.

الحالة	ما يحدث
طلبت رمزًا جديدًا	لكل حساب رمز فعّال واحد: يصبح الرمز السابق غير صالح.
أدخلت الرمز خطأ	بعد **5** محاولات خاطئة في المجموع يصبح الرمز غير صالح ولا يُصدَر رمز جديد مدة **15 دقيقة**. طلب رمز جديد لا يصفّر العدّاد.
لم يصل الرمز	تبدو الشاشة نفسها حتى لو لم يكن الحساب الذي كتبته موجودًا (لا يُكشف وجود الحساب من عدمه). اسأل المسؤول عن اسم المستخدم والبريد / الهاتف المسجَّل في الحساب.

> **إن كنت تستخدم قالبًا مخصّصًا** إذا كان قالب بريد أو SMS إعادة تعيين كلمة المرور لديك يذكر «رمزًا من 6 أرقام» فصحّح النص: الرمز من 8 أرقام اعتبارًا من 3.10.1.

تُغلق الجلسات الأخرى عند تغيّر كلمة المرور

عندما تغيّر كلمة مرورك بنفسك، أو يعيد Root تعيينها، أو تُجدَّد عبر «نسيت كلمة المرور» أو عبر دعوة، تُغلق **جلسات الحساب في المتصفحات الأخرى** و**جلسات الهاتف (تطبيق الجوال)** و**رموز MCP**. تبقى الجلسة التي أجرت التغيير مفتوحة؛ وتُبلَّغ على الشاشة بعدد جلسات الهاتف ورموز MCP التي أُغلقت.

سجّل الدخول إلى التطبيق على الهاتف من جديد.

رموز MCP **تُحذف**: أنشئ رمزًا جديدًا من صفحة **MCP (الذكاء الاصطناعي)** لعميل الذكاء الاصطناعي الخارجي (مثل Claude Desktop).

عند حذف مستخدم تُحذف أيضًا جلسات هاتفه ورموز MCP ومفاتيح الوصول إلى البيانات الخاصة به.

تغيير البريد الإلكتروني أو الهاتف يتطلب كلمة المرور

في نافذة **ملفي الشخصي** يظهر سطر **كلمة مرورك الحالية** عندما تغيّر البريد الإلكتروني أو الهاتف؛ ولا يُحفظ التغيير من دون كلمة المرور. في **الإنذارات ← إشعارات الإنذار الخاصة بي** تُسأل عن كلمة مرورك الحالية عند الضغط على «حفظ» إذا كان البريد أو الهاتف يتغيّر. إذا لم تتغيّر القيمة (مربعات الإشعار فقط) فلا تُطلب كلمة المرور. السبب: ألّا يُغيَّر عنوان الاسترداد من حاسوب تُركت جلسته مفتوحة فيُستولى على الحساب.

اسم المستخدم والدعوة وقفل تسجيل الدخول

الموضوع	القاعدة
اسم المستخدم	لا يمكن إنشاء حساب ثانٍ باسم لا يختلف إلا في حالة الأحرف ("ilker" / "İlker"، "ömer" / "Ömer")؛ ولا يمكن إعادة تسمية حساب إلى اسم كهذا.
الدعوة	المستخدم غير Root لا يستطيع دعوة إلا مستخدم دوره أدنى من دوره. الدعوة تغلق الجلسات المفتوحة للحساب المدعوّ. عنوان تسجيل الدخول في البريد يؤخذ من حقل **العنوان العام (URL عام)**.
قفل تسجيل الدخول	بعد 8 محاولات خاطئة خلال 5 دقائق يُقفل الحساب 5 دقائق (HTTP 429). يُطبَّق الحد نفسه لكل اسم مستخدم على تسجيل الدخول باسم المستخدم / كلمة المرور (Basic) في REST API.

انظر أيضًا الأدوار والصلاحيات · رمز MCP

HTTPS / النشر العام

الإعدادات ← الويب وREST API والجوال: تبويب **الشهادة** (توليد شهادة موقّعة ذاتيًا أو رفع PFX)، وتبويب **النشر وHTTPS** (اختيار الحالة والخطوات، ومنفذ HTTPS، وإعادة التوجيه من HTTP إلى HTTPS، والعنوان العام، والتحقق). الشرح خطوة بخطوة: النشر على الويب. عند الإتاحة على الإنترنت: اجعل عنوان الاستماع `0.0.0.0`، ووجّه DNS إلى الخادم، وافتح منافذ جدار الحماية، وعطّل AllowAnonymous، وكلمة المرور القوية إلزامية. تُطبَّق التغييرات عند إعادة التشغيل.

العمل خلف وكيل عكسي (الوسطاء الموثوقون)

إذا كان أمام الخادم وكيل عكسي (IIS أو nginx أو موازن أحمال) فإن عنوان العميل الحقيقي وكون الاتصال عبر HTTPS تخبر بهما الترويسات `X-Forwarded-For` و `X-Forwarded-Proto` و `X-Forwarded-Host` التي يضيفها الوكيل. اعتبارًا من 3.10.1 لا تُقبل هذه الترويسات **إلا من وكيل موثوق** (كانت تُقبل من أي جهة: فكان يمكن تزوير عنوان العميل ومعلومة «جئت عبر HTTPS»).

أين الوكيل	ما العمل
على الحاسوب نفسه (IIS أو nginx أو cloudflared)	لا شيء. الوكيل الموجود على هذا الحاسوب موثوق دائمًا.

على جهاز آخر	في تبويب **الإعدادات** ← **الويب وREST API والجوال** ← **النشر وHTTPS** (المسار C، «أين خادم الويب؟» = على حاسوب آخر) اكتب عنوان الوكيل في حقل **الوسطاء الموثوقون**: عنوان IP واحد أو شبكة CIDR واحدة في كل سطر (مثل `10.0.0.5` أو `10.0.0.0/24`). احفظ ثم **أعد تشغيل الخدمة**. العنوان غير الصالح لا يُحفظ؛ وتذكر الرسالة السطر غير الصالح.
وكيل سحابي يتصل بالخادم مباشرة	اكتب نطاقات عناوين المزوّد. لا يلزم ذلك إن كنت تستخدم نفق `cloudflared` (فالنفق محلي).

الأعراض بعد الترقية. إذا كان الوكيل على جهاز آخر والحقل فارغًا: يظهر في سجل التدقيق وفي المستخدمين النشطين عنوان الوكيل بدل عنوان العميل؛ وإذا كان «إعادة توجيه HTTP إلى HTTPS» مفعّلًا فقد تدخل الصفحة في إعادة توجيه لا تنتهي؛ وقد يُرفض مفتاح الوصول إلى البيانات (`mhkey_`) بحجة «HTTPS فقط». الحل هو الحقل أعلاه.

العنوان العام (URL عام) (في صفحة MCP (الذكاء الاصطناعي)) إعداد مستقل: يُشتق منه عنوان تسجيل الدخول في رسائل الدعوة والإعلان وعناوين الذكاء الاصطناعي / MCP. ولا يلزم لفحص الأصل أدناه.

طلب صادر من موقع آخر (فحص الأصل)

إذا حاولت صفحة في موقع آخر تنفيذ عملية باسمك وجلستك مفتوحة رفض الخادم الطلب بالرمز 403. يُتَّخذ القرار بحسب الأصل الذي يبلّغ عنه المتصفح؛ ولا تتأثر بذلك تثبيتات الوكيل العكسي ولا السكربتات. المتصفحات لا ترسل هذه المعلومة إلا في عناوين **HTTPS** و `localhost` : فإذا فتحت الواجهة عبر HTTP العادي بعنوان IP لم يعمل هذا الفحص. فعّل HTTPS للحماية الكاملة.

تحصين الخادم: قفل مجلد البيانات، كلمة مرور النسخ الاحتياطي، تشفير القرص

الإصدار `3.11.0`

يحتفظ MergenHub بكل بياناته في **مجلد البيانات** على الخادم: `C:\ProgramData\MergenHub` . وفيه المستخدمون والصلاحيات، والمشروع، والإعدادات (كلمة مرور البريد الإلكتروني / SMS، ومفاتيح الاتصال)، والسجلات، والشهادات، والنسخ الاحتياطية. ملفات قاعدة البيانات غير مشفّرة بكاملها؛ لكن **كلمات المرور التي بداخلها مشفّرة** (انظر «كلمات المرور المحفوظة تُخزَّن مشفّرة» أدناه). يشرح هذا القسم كيف تحدّ من وصول من يستطيع بلوغ الخادم إلى هذه الملفات عبر **ثلاثة تدابير منفصلة**. الثلاثة كلها **اختيارية** ولا يُفعَّل أيٌّ منها من تلقاء نفسه. أما تشفير كلمات المرور المحفوظة فمفعَّل دائمًا ولا يطلب منك أي إجراء.

التهديد	التدبير	أين
ملف الإعدادات أو قاعدة البيانات يقع في يد أحد **وحده** (ملف أُرسل إلى الدعم، ملف منسوخ)، أو مستخدم ليس مسؤولًا يفتح ملف الإعدادات	**تشفير كلمات المرور المحفوظة** (مفعَّل دائمًا)	تلقائيًا. الحالة: الإعدادات ← الأمان ← كلمات المرور المحفوظة
مستخدم Windows يستطيع تسجيل الدخول إلى الخادم و**ليس مسؤولًا** يفتح الملفات ويقرؤها	**قفل مجلد البيانات**	الإعدادات ← الأمان ← حماية مجلد البيانات (أو معالج التثبيت)
ملف نسخة احتياطية يخرج من الخادم: مشاركة شبكة، مرفق بريد إلكتروني، قرص يُنقل إلى مكان آخر	**كلمة مرور النسخ الاحتياطي**	الإعدادات ← نسخ احتياطي ← كلمة مرور النسخ الاحتياطي
قرص الخادم يُسرق أو يُنزع، أو يُحال الخادم إلى الخردة	**تشفير القرص** (BitLocker)	في Windows؛ MergenHub لا يقوم بذلك بنفسه
شخص له صفة **المسؤول** في Windows يفتح الملفات أو يغيّرها	لا يستطيع التطبيق منع ذلك. حدّ ممّن لهم صفة المسؤول.	في Windows

الحالة الافتراضية إذا لم تختر شيئًا بعد التثبيت: يستطيع كل مستخدم Windows على الخادم قراءة مجلد البيانات (هذا هو الإذن الافتراضي في Windows للمجلد `ProgramData`)، والنسخ الاحتياطية ملفات zip عادية. أما مجلدات الشهادات والنسخ الاحتياطية وسجل الإصدارات ومفتاح الخدمة فمتاحة دائمًا للمسؤولين فقط. كلمات مرور المستخدمين لا تُخزَّن في الملف نصًّا عاديًا (تُخزَّن على هيئة تجزئة)؛ وكذلك كلمة مرور البريد الإلكتروني / SMS ومفاتيح الاتصال وكلمات مرور برامج التشغيل تُخزَّن مشفّرة (منذ الإصدار 3.12.0؛ كانت الإصدارات السابقة تخزّنها نصًّا عاديًا).

كلمات المرور المحفوظة تُخزَّن مشفّرة

الإصدار 3.12.0

كلمات المرور التي تُدخلها في MergenHub لا تُحفظ نصًّا عاديًا في الملفات وقاعدة البيانات؛ بل تُشفَّر بخوارزمية **AES-256**. النطاق: كلمة مرور البريد الإلكتروني و SMS (ومع مزوّد SMS العام قالب العنوان والنص أيضًا: فالمفتاح يكون فيهما غالبًا)، مستخدمو OPC UA، كلمات مرور ورموز وكلاء جسر البيانات، مفاتيح الذكاء الاصطناعي، اتصالات مصادر البيانات وتسجيل البيانات (كلمة المرور وسلسلة اتصال ODBC كاملة)، كلمات مرور برامج التشغيل (MQTT، عميل OPC UA، IEC 61850...)، مفاتيح webhook والترويسات في مسارات الأتمتة، كلمة مرور النسخ الاحتياطي وكلمة مرور شهادة HTTPS. أما ملفات سجل إصدارات الإعداد وملفات المشروع المحفوظة عبر API (المجلد projects) فتُشفَّر بكاملها.

لا يُطلب منك أي إجراء. تُدخل كلمات المرور كالمعتاد؛ ولا تتغيّر الواجهة ولا API (تظهر كلمات المرور مقنَّعة كما كانت). إذا رقّيت من إصدار سابق فإن كلمات المرور التي تركها ذلك الإصدار نصًّا عاديًا تُشفَّر مرة واحدة عند أول تشغيل للخدمة، ويُضاف إلى سجل الأحداث السطر "Kayıtlı parolalar şifrelendi" (تم تشفير كلمات المرور المحفوظة).

رؤية الحالة (لمستخدم Root فقط). بطاقة **كلمات المرور المحفوظة** في أسفل صفحة **الإعدادات** ← **الأمان** تعرض "كلمات المرور المحفوظة مشفّرة" واسم ملف المفتاح. وإذا وُجدت مشكلة تذكر البطاقة نفسها السبب: "تعذّر فتح بعض كلمات المرور المحفوظة"، أو أسماء الملفات التي ما زالت تحتوي على كلمات مرور بنص عادي.

أين المفتاح؟ كل تثبيت ينشئ مفتاحه العشوائي الخاص؛ والمفتاح غير مضمَّن في البرنامج. ملفه في مجلد البيانات: `C:\ProgramData\MergenHub\keys\secrets-XXXXXXXX.key` (XXXXXXXX هو معرّف المفتاح). وحتى لو كان قفل مجلد البيانات متوقفًا، لا يقرأ المجلد `keys` سوى **SYSTEM** و **Administrators**. **لا تحذف هذا الملف ولا تغيّره.**

السؤال	الجواب
ممَّ يحمي؟	من مستخدم Windows ليس مسؤولًا يستطيع قراءة ملف الإعدادات أو قاعدة البيانات لكنه لا يستطيع قراءة مجلد المفاتيح؛ ومن ملف وقع في يد أحد وحده (ملف إعدادات أُرسل إلى الدعم، قاعدة بيانات منسوخة)؛ وممن يتصفح محتوى نسخة احتياطية بلا كلمة مرور.
ممَّ لا يحمي؟	من مسؤول Windows، وممن يحصل على مجلد البيانات **كاملًا** أو على **نسخة احتياطية كاملة بلا كلمة مرور**: فالمفتاح بداخلها أيضًا. لهؤلاء استخدم كلمة مرور النسخ الاحتياطي وتشفير القرص (أدناه).
إذا استعدت النسخة الاحتياطية على خادم آخر، هل أُدخل كلمات المرور من جديد؟	لا. النسخة الاحتياطية تتضمن المجلد `keys` أيضًا؛ فتُفتح كلمات المرور تلقائيًا على الخادم الجديد. ولا يُحذف مفتاح الخادم الجديد: يبقى ملفا المفتاحين جنبًا إلى جنب في المجلد.
نسخت ملف الإعدادات أو قاعدة البيانات فقط إلى خادم آخر	يتعذّر فتح كلمات المرور في ذلك الملف: يظهر في الشريط العلوي وفي بطاقة **كلمات المرور المحفوظة** التحذير "تعذّر فتح بعض كلمات المرور المحفوظة"، ولا تعمل الاتصالات التي تستخدم تلك الكلمات (لا يُحاوَل الاتصال أصلًا: القيمة التي يتعذّر فتحها لا تُرسَل إلى النظام المقابل ككلمة مرور). انسخ أيضًا الملفات الموجودة في المجلد `keys` على الخادم القديم إلى المجلد `keys` على الخادم الجديد ثم أعد تشغيل الخدمة، أو أدخل كلمات المرور من جديد. لا تُحذف كلمات المرور؛ تُفتح تلقائيًا عند وصول المفتاح.
ماذا لو حُذف ملف المفتاح؟	يتعذّر فتح كلمات المرور المشفّرة بذلك المفتاح ويجب إدخالها من جديد. المفتاح موجود أيضًا داخل نسخك الاحتياطية: يمكنك إعادته منها.
ماذا لو اضطررت إلى العودة إلى إصدار أقدم (3.11.0 وما قبله)؟	الإصدار الأقدم لا يستطيع قراءة القيم المشفّرة. **قبل** العودة، والخدمات متوقفة، حوّل كلمات المرور إلى نص عادي من موجّه أوامر بصلاحية المسؤول (الأمر أدناه).
ماذا لو اخترت "تضمين بيانات الاعتماد" في حزمة المشروع؟	تحمل الحزمة كلمات المرور نصًّا عاديًا ليمكن استيرادها في نظام آخر. هذا اختيارك الصريح؛ فاحفظ الحزمة على هذا الأساس.
وماذا عن النسخ الاحتياطية المأخوذة قبل الترقية؟	تبقى كما هي: ملف الإعدادات وقاعدة البيانات بداخلها على حالهما يوم أُخذت، أي أن كلمات المرور فيها نص عادي. احذف ما لا تحتاج إليه منها أو انقله إلى مكان آمن؛ وخذ نسخة احتياطية جديدة بعد الترقية.
ما الذي لا يُشفَّر؟	السجلات وسجلات الأحداث والتدقيق ومحادثات المساعد نص حر. لا تكتب كلمات مرور في حقول الوصف والملاحظات والرسائل.

سطر الأوامر (من موجّه أوامر بصلاحية **المسؤول** على الخادم):

```
"C:\Program Files\MergenHub\MergenHub.exe" secrets status
"C:\Program Files\MergenHub\MergenHub.exe" secrets decrypt
"C:\Program Files\MergenHub\MergenHub.exe" secrets encrypt
```

`status` يبيّن هل المفتاح في مكانه وما الملفات التي ما زالت تحتوي على كلمات مرور بنص عادي. `decrypt` يحوّل كل كلمات المرور إلى نص عادي: استخدمه فقط قبل العودة إلى إصدار أقدم، والخدمات متوقفة. `encrypt` يشفّر ما بقي نصًّا عاديًا فورًا (الخدمة تفعل ذلك أصلًا عند كل تشغيل).

1. قفل مجلد البيانات

يفتح القفل مجلد البيانات لحسابَي **SYSTEM** و**Administrators** فقط. مستخدمو Windows غير المسؤولين لا يستطيعون فتح أي ملف في المجلد. القفل **غير مفعَّل افتراضيًا**؛ وتفعيله قرارك أنت.

تحقّق قبل تفعيله

حساب الخدمة. تُثبَّت خدمات MergenHub لتعمل بحساب SYSTEM؛ وفي هذه الحالة لا يؤثّر القفل فيها. إذا غيّرت حساب الخدمة *يدويًا* فامنح ذلك الحساب أولًا التحكم الكامل في مجلد البيانات، وإلا فقد يتعذّر بدء الخدمة.

برامج أخرى تقرأ المجلد. إذا كان وكيل نسخ احتياطي أو برنامج مراقبة يقرأ المجلد بحساب ليس مسؤولًا فلن يستطيع قراءته بعد القفل. امنح ذلك الحساب إذن القراءة على المجلد يدويًا؛ فالقفل **يُبقي** الأذونات التي منحتها يدويًا لحساب محدّد ولا يزيل إلا إذن المجموعات الواسعة مثل «Users».

الدعم. جمع ملفات السجل (`logs`) يتطلب الآن صلاحيات المسؤول: يسأل مستكشف الملفات «Continue» عند دخول المجلد.

تفعيله من الواجهة (للمستخدم Root فقط)

افتح صفحة **الإعدادات** ← **الأمان**. في أسفل الصفحة تعرض بطاقة **حماية مجلد البيانات** الحالة: «القفل غير مفعَّل» أو «القفل مفعَّل»، ومسار المجلد، وجدول **من يستطيع الوصول إلى المجلد حاليًا**. إذا كان في الجدول صف موسوم بعبارة «مجموعة واسعة» (مثل `BUILTIN\Users`) فإن المستخدمين غير المسؤولين يستطيعون قراءة المجلد.

اضغط زر **قفل المجلد...**. النافذة التي تُفتح تبيّن ما الذي يتغيّر، ومن يتأثّر، وما الذي قد يتعطّل، وما الذي لا يحمي منه القفل، وكيف يُتراجع عنه. اقرأها كاملة.

حدّد **المربعات الثلاثة** كلها أسفلها واضغط **قرأته، متابعة**. لا يمكن المتابعة قبل تحديد المربعات.

في نافذة **التأكيد النهائي** اكتب في المربع **اسم الخادم** الظاهر على الشاشة واضغط **قفل**. إذا لم يتطابق الاسم لا يُنفَّذ شيء (كي لا يُؤكَّد القفل على خادم خاطئ أو بحكم العادة).

تتحوّل البطاقة إلى «القفل مفعَّل»؛ ولا تبقى في الجدول أي مجموعة واسعة. وتُكتب العملية في سجل التدقيق.

تفعيله أثناء التثبيت. في معالج التثبيت صفحة **حماية مجلد البيانات**؛ ومربع «قفل مجلد البيانات — يقرؤه SYSTEM و Administrators فقط» يأتي **غير محدّد**. إذا حدّدته عُرضت التحذيرات نفسها عند الضغط على «التالي» وسُئلت مرة أخرى (الزر الافتراضي هو «لا»). وإذا لم تحدّده لا تُمسّ الأذونات؛ وإن كان المجلد مقفلًا من قبل بقي مقفلًا. في التثبيت الصامت يُفعَّل القفل بالمعامل `/LOCKDATA=1` .

إزالة القفل. في البطاقة نفسها: **إزالة القفل...** ← حدّد المربع ← اكتب اسم الخادم ← **إزالة القفل**. يرث المجلد أذونات `ProgramData` من جديد: يستطيع كل مستخدم Windows على الخادم قراءة الملفات مجددًا.

إذا تعذّر الوصول إلى الواجهة (مثلًا إذا لم تبدأ الخدمة)، فمن موجّه أوامر بصلاحيات **المسؤول** على الخادم:

```
"C:\Program Files\MergenHub\MergenHub.exe" data-lock status
"C:\Program Files\MergenHub\MergenHub.exe" data-lock off
"C:\Program Files\MergenHub\MergenHub.exe" data-lock on
```

`status` يطبع الحالة، و `off` يزيل القفل، و `on` يقفل (يؤدي العمل نفسه الذي يؤديه الزر في الواجهة؛ ولا يعرض أي تحذير).

السؤال	الجواب
هل تواصل أيقونة شريط النظام وتطبيق سطح المكتب العمل؟	نعم. يقرآن عنوان الواجهة من ملف منفصل لا يحتوي أسرارًا (`public\shell.json`)؛ ويبقى ذلك الملف مقروءًا للجميع.
هل تُبطل الترقية القفل؟	لا. لا يمسّ التثبيت الأذونات ما لم تحدّد المربع.
هل يحمي القفل من مسؤول Windows؟	لا. يستطيع المسؤول فتح كل ملف، وتغيير الأذونات أيضًا.
ماذا لو كان مجلد النسخ الاحتياطية في مكان آخر؟	يشمل القفل مجلد البيانات فقط. أذونات مجلد النسخ الاحتياطية الموجود على مشاركة شبكة أو على قرص آخر تديرها أنت؛ استخدم **كلمة مرور النسخ الاحتياطي** للملفات هناك.
الخدمة لا تبدأ بعد القفل	ربما غُيِّر حساب الخدمة يدويًا. أزل القفل بالأمر `data-lock off` من موجّه أوامر بصلاحيات المسؤول، وامنح الحساب التحكم الكامل في المجلد، ثم اقفل من جديد.

2. كلمة مرور النسخ الاحتياطي

يحتوي ملف النسخة الاحتياطية على حسابات المستخدمين وإعدادات الخادم وكلمات مرور الاتصالات المحفوظة. إذا لم تُحدَّد كلمة مرور كُتبت النسخة الاحتياطية **ملف zip عاديًا**: كل من يحصل على الملف يستطيع قراءة ما بداخله. كلمات المرور المحفوظة بداخله مشفّرة، لكن مفتاحها موجود داخل النسخة أيضًا لكي يمكن فتحها على خادم آخر؛ ومن يحصل على النسخة كاملة ويُصرّ يستطيع فتحها. وإذا حدّدت كلمة مرور كُتبت النسخة الاحتياطية مشفّرة (امتدادها `.mhbak`) ولا يمكن فتحها دون كلمة المرور؛ وتكون النسخة التي تذهب إلى مشاركة شبكة أو مرفق بريد إلكتروني أو قرص آخر محمية أيضًا.

في صفحة **الإعدادات** ← **نسخ احتياطي** انتقل إلى قسم **كلمة مرور النسخ الاحتياطي (اختياري)**.
اكتب كلمة المرور نفسها في الحقلين **كلمة المرور** و**كلمة المرور (مرة أخرى)** (8 أحرف على الأقل) واضغط **حفظ**.
اقرأ التحذير الذي يظهر، وبعد أن تدوّن كلمة المرور في مكان آمن خارج الخادم اضغط **نعم دوّنتها، حفظ**.
النسخ الاحتياطية المأخوذة من الآن فصاعدًا تظهر في القائمة بأيقونة قفل وبالامتداد `.mhbak` . أما النسخ الاحتياطية المأخوذة سابقًا فتبقى كما هي.

> **إذا نُسيت كلمة المرور** لا يمكن فتح النسخة الاحتياطية؛ ولا توجد وسيلة لاستعادتها، ولا تستطيع Envest فتحها أيضًا. احفظ كلمة المرور في مكان آمن خارج الخادم.

فتح نسخة احتياطية محمية بكلمة مرور. هناك طريقتان:

من الواجهة: الإعدادات ← نسخ احتياطي ← **فك التشفير والتنزيل** في صف النسخة الاحتياطية ← اكتب كلمة المرور ← **فك التشفير والتنزيل**. يُنزَّل ملف zip عادي إلى المتصفح. تُستخدم كلمة المرور لذلك الطلب فقط ولا تُخزَّن.

من سطر الأوامر (إذا كان الخادم لا يعمل أو نُقلت النسخة الاحتياطية إلى جهاز آخر؛ ويجب أن يكون MergenHub مثبّتًا على ذلك الجهاز):

```
"C:\Program Files\MergenHub\MergenHub.exe" backup-decrypt MergenHub-yedek-20261116-020000.mhbak
yedek.zip
```

يطلب الأمر كلمة المرور (لا تظهر على الشاشة) ويكتب ملف zip العادي.

خطوات الاستعادة هي نفسها في النسخة الاحتياطية العادية: فكّ تشفير النسخة الاحتياطية أولًا، ثم أوقف الخدمة واستخرج ملف zip إلى مجلد البيانات. انظر النقل مع السجل التاريخي والنسخ الاحتياطي الكامل للنظام.

> **أين تُحفظ كلمة المرور؟** لأن النسخ الاحتياطي المجدول يعمل دون مراقبة، تُخزَّن كلمة المرور في ملف إعدادات الخادم **مشفّرة** مثل بقية كلمات المرور المحفوظة. من يستطيع قراءة مجلد المفاتيح (مسؤول Windows) يستطيع فتح كلمة المرور؛ أما المستخدمون غير المسؤولين فلا يستطيعون. كلمة مرور النسخ الاحتياطي تحمي الملف الذي **يخرج من الخادم**؛ أما بقية الملفات داخل الخادم فاستخدم لها قفل مجلد البيانات. الواجهة و API لا تعرضان كلمة المرور أبدًا.

إزالة كلمة المرور. أفرغ الحقلين واضغط **حفظ**؛ ثم أكّد التحذير. تصبح النسخ الاحتياطية اللاحقة ملفات zip عادية. والنسخ الاحتياطية المحمية بكلمة مرور المأخوذة سابقًا يبقى فتحها ممكنًا بكلمة المرور القديمة.

3. تشفير القرص (BITLOCKER)

قفل مجلد البيانات وأذونات Windows لا تسري إلا ما دام Windows يعمل. إذا نُزع القرص من الخادم ورُكِّب في جهاز آخر لم يعد للأذونات أي معنى: يمكن قراءة الملفات. والحماية الوحيدة من ذلك هي تشفير القرص. MergenHub لا يقوم بذلك بنفسه؛ استخدم ميزة **BitLocker** في Windows.

في Windows Server أضف ميزة **تشفير محرك الأقراص BitLocker**؛ وفعّلها على محرك الأقراص الذي يحتوي مجلد البيانات (غالبًا `C:`).

إذا كنت تكتب النسخ الاحتياطية إلى قرص آخر أو إلى قرص قابل للإزالة فشفّر ذلك القرص أيضًا أو استخدم كلمة مرور النسخ الاحتياطي.

احفظ **مفتاح الاسترداد** خارج الخادم. إذا فُقد المفتاح تعذّر الوصول إلى البيانات الموجودة على القرص.

في الأجهزة الافتراضية يجب أن يُحمى بالطريقة نفسها التخزين الذي يحتوي القرص الافتراضي ونسخته الاحتياطية.

4. من ينبغي أن يكون مسؤولًا؟

من له صفة المسؤول في Windows يستطيع فتح مجلد البيانات، وإزالة القفل، وتغيير قاعدة البيانات ومنح نفسه صلاحيات، وإيقاف الخدمة. ولهذا لا يكون للتدابير الثلاثة أعلاه معنى إلا إذا كانت حسابات المسؤول على الخادم قليلة وخاضعة للرقابة.

استخدم حسابًا غير مسؤول للعمل اليومي على الخادم؛ واستخدم حسابات المسؤول للصيانة فقط.

إذا لم يكن المشغّلون بحاجة إلى تسجيل الدخول إلى Windows على الخادم فلا تسمح لهم بذلك: يستخدمون MergenHub من المتصفح أو من تطبيق سطح المكتب على حواسيبهم، بحساباتهم الخاصة في MergenHub.

افتح الوصول عبر سطح المكتب البعيد (RDP) للأشخاص والشبكات التي تحتاج إليه فقط.

انظر أيضًا الأدوار والصلاحيات · النسخ الاحتياطي الكامل للنظام · النشر على الويب و HTTPS