أسس
OSOS

توثيق أسس

الإدارة

قسم من مركز التوثيق والمساعدة في أسس

النسخة العربية

إصدار المنصّة 1.10
تاريخ النشر: 23 نوفمبر 2026

الأدلة · الإرشادات

المحتويات

ابدأ من هنا: الإدارة 3

الأدلة

إدارة المستخدمين 5
إدارة المجموعات 11
إدارة الأدوار 15
الوحدات التنظيمية 19
الأذونات والوصول 22
الأذونات الحساسة 29
التفويض 38
إعدادات المنظمة 43
ساعات العمل والعطلات 48
المساحات والنطاقات 52
التحقق البشري (الحماية من الروبوتات) 55
المظهر: السمات والخطوط والأيقونات 58
المراقبة: السجلات والتدقيق 61
الإشعارات وقوالب البريد الإلكتروني 66
رخصتك وحدود خطتك 70
المستخدمون من دليل شركتك 71
طرق تسجيل الدخول والدخول الموحّد 75

الإرشادات

إدارة الأذونات 83
اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط 86
أنشئ رمز API لعملية تكامل 89

Videos

فيديو: إدارة الأذونات (بما فيها الحقول الحساسة) 92
أسئلة الإدارة الشائعة 93

ابدأ من هنا: الإدارة

هذا القسم موجّه إلى **مسؤولي القاطن**، أي من يتولّون تشغيل أسس لمؤسستهم يوميًا. فأنت من يقرّر طريقة تسجيل الدخول، وكيف تُنظَّم مؤسستك، وما يُسمح لكل شخص بفعله، وكيف تبدو المنصة وكيف تتواصل مع مستخدميها. وتنجز ذلك كلّه داخل المنتج، من قائمة **الإدارة**، دون أن تحتاج إلى تثبيت خوادم أو ضبطها.

تستند الأمثلة في هذا القسم كلّه إلى قسم الموارد البشرية في شركة متوسطة الحجم: مجموعة **الموارد البشرية**، ودور **مدير الموارد البشرية**، وخدمات للموارد البشرية مثل طلبات الإجازة.

قبل أن تبدأ

تتطلّب معظم شاشات الإدارة أن يكون مستوى صلاحيتك على النظام **إدارة**؛ إذ لا تظهر **المنظمة** و**إدارة الوصول** في القائمة من دونه. فإن لم تجدهما، فاطلب ممّن أعدّ لك المنصة أن يمنحك مستوى **إدارة**. راجع الأذونات والوصول.

قائمة الإعداد في يومك الأول

اتّبع هذه الخطوات بالترتيب؛ فكل خطوة تعتمد على ما قبلها.

1. **اختر طريقة تسجيل الدخول.** حدّد ما ستعتمده من كلمات المرور ومفاتيح المرور والمصادقة الثنائية، وقرّر ما إذا كان الموظفون سيسجّلون الدخول بحسابات شركتك (الدخول الموحّد). ← طرق تسجيل الدخول والدخول الموحّد
2. **أعدّ المساحات والهيكل التنظيمي.** أنشئ مساحاتك أولًا، ثم الإدارات والوحدات في الهيكل التنظيمي. ← المساحات والنطاقات · الوحدات التنظيمية
3. **أنشئ الأدوار والمجموعات.** الأدوار للمناصب (*مدير الموارد البشرية*)، والمجموعات للفرق (*الموارد البشرية*). ← إدارة الأدوار · إدارة المجموعات
4. **أضف المستخدمين.** أضِفهم واحدًا تلو الآخر، أو اطلب من المشغّل استيرادهم من دليل شركتك، ثم أسندهم إلى الأدوار وأضِفهم إلى المجموعات. ← إدارة المستخدمين · المستخدمون من دليل شركتك
5. **امنح الوصول.** امنح كل شخص مستوى أساسيًا، ثم امنح كل مجموعة وكل دور ما يتطلّبه العمل من أذونات. ← الأذونات والوصول · إدارة الأذونات
6. **اجعل المنصة تحمل هوية مؤسستك.** اضبط الشعار والألوان والخطوط واللغات والمنطقة الزمنية وصيغ التاريخ. ← إعدادات المنظمة · الواجهات والمظهر
7. **اضبط الإشعارات.** أعدّ قوالب البريد الإلكتروني والرسائل، وبيانات المرسِل، وقنوات الإرسال. ← إعداد الإشعارات
8. **اعرف أين تبحث حين يقع خلل.** راجع سجلات الرسائل، وسجل التدقيق، وسجلات الأتمتة. ← المراقبة: السجلات والتدقيق

المهام الشائعة

- امنح مجموعة وصولًا إلى وحدة أو كيان أو معرض أو تقرير
- اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط
- تحقّق مما يستطيع شخص ما الوصول إليه

- اسمح لمديري الموارد البشرية وحدهم برؤية الرواتب
- اسمح لشخص بالعمل نيابةً عن زميله في أثناء غيابه
- اضبط ساعات العمل والعطلات
- راجع رخصتك وحدود خطتك

ألديك أسئلة لم تجد إجابتها هنا؟ جرّب الأسئلة الشائعة حول الإدارة.

ما ليس من مهامك

بعض الأمور تُضبط خارج **الإدارة**، ويتولّاها أشخاص آخرون:

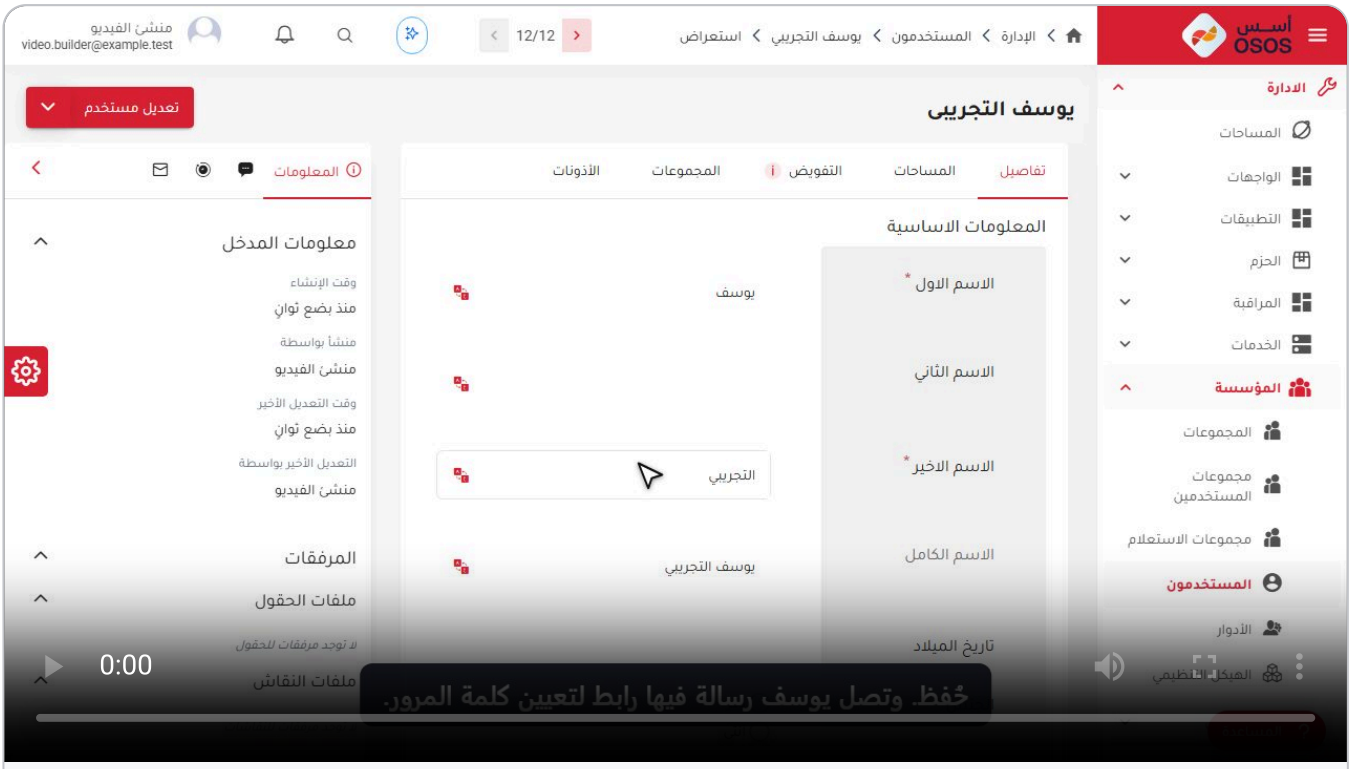
المهمة	من يتولّاها
تثبيت المنصة وترقيتها ونسخها احتياطيًا، والخوادم والشبكات والشهادات	**المشغّل** لديك (الفريق الذي يدير المنصة)
ضبط خادم الهوية، وتسجيل مزوّدي الدخول الموحّد، وتشغيل عمليات الاستيراد من الدليل	**المشغّل** لديك؛ فأنت تحدّد المطلوب وتزوّده بالتفاصيل
رخصتك وخطتك	**المورّد** أو المشغّل
تصميم التطبيقات وكيانات البيانات والمعارض والصفحات والخدمات وسير العمل	**بُناة التطبيقات** لديك – راجع قسم التطوير [بناء التطبيقات › بناء التطبيقات – ابدأ من هنا]

وحين تحتاج إلى أحد هذه الأمور، أخبر الشخص المعنيّ بما تحتاجه بلغة العمل، كأن تقول: «يجب أن يسجّل الموظفون الدخول بحسابات العمل على Microsoft»، أو «استورِد كل موظفي قسم الموارد البشرية».

> **للتعمّق أكثر**
>
> للمشغّلين: نظرة عامة على الإعداد · النشر · تجهيز القاطنين

إدارة المستخدمين

هذا الدليل موجّه إلى مسؤولي القاطن، ويبيّن لك كيفية إضافة الأشخاص إلى أسس، وتجهيز المستخدم الجديد لبدء العمل، وإدارة حسابه يوميًا، وإغلاقه على نحو سليم عند مغادرته. ويتناول أيضًا **مستخدمي التطبيقات**، أي الحسابات التي تستخدمها الأنظمة الخارجية لاستدعاء أسس.



إرشاد **أضف مستخدمًا** زميل جديد، جاهز لتسجيل الدخول – 0:40 – سُجِّل على أسس 1.11.0-alpha.1

تتابع الأمثلة ما يجري في إدارة الموارد البشرية: تنضم لينا إلى الإدارة بصفتها موظفة موارد بشرية، ثم يغادر عمر الشركة لاحقًا.

كيف تعمل

كل شخص في أسس هو مُدخل في قائمة **المستخدمون**. وعندما تحفظ مستخدمًا جديدًا، يُنشئ أسس حساب تسجيل الدخول الخاص به نيابةً عنك، ويرسل إليه بالبريد الإلكتروني رابطًا لتعيين كلمة مروره بنفسه، دون أن تطّلع عليها أو تضبطها بنفسك أبدًا.

يتيح مُدخل المستخدم وحده للشخص تسجيل الدخول، ولا يكاد يتيح له شيئًا آخر: أما ما يستطيع رؤيته وفعله، فتحدّده:

- **مستوى صلاحيته على النظام** (يحتاج كل شخص إلى **مقيّد** على الأقل)،
- و**المجموعات** التي ينتمي إليها و**الأدوار** التي يشغلها في الهيكل التنظيمي،
- و**المساحات** التي هو عضو فيها.

لذا تتطلب إضافة شخص دائمًا خطوتين: إنشاء المستخدم، ثم تجهيزه.

وهناك نوعان من المستخدمين:

نوع المستخدم	لمن هو	كيف يسجّل الدخول
طبيعي	لشخص.	بكلمة مرور، أو مفتاح مرور، أو الدخول الموحّد، بحسب إعدادات تسجيل الدخول لديك.
تطبيق	لنظام خارجي، مثل نظام للموارد البشرية أو المالية يرسل البيانات إلى أسس.	برمز API، ولا يستخدم صفحة تسجيل الدخول أبدًا.

ويمكن أيضًا جلب الأشخاص من دليل شركتك بدلًا من إضافتهم يدويًا. راجع المستخدمون من دليل شركتك.

قبل أن تبدأ

- تحتاج إلى مستوى **إدارة** على النظام؛ فمن دونه لا تظهر قائمة **المنظمة**.
- يحتاج الشخص إلى اسم مستخدم فريد وعنوان بريد إلكتروني فريد، إذ يُرسل رابط تعيين كلمة المرور إلى هذا العنوان.

إضافة مستخدم

مثال: إضافة لينا، موظفة الموارد البشرية الجديدة.

1. افتح **الإدارة › المنظمة › المستخدمون**.
2. اختر **إضافة مستخدم**.
3. في **المعلومات الاساسية**، أدخل **الاسم الاول** و**الاسم الاخير** (و**الاسم الثاني** إن وُجد). يُملأ **الاسم الكامل** تلقائيًا، ويمكنك إضافة **تاريخ الميلاد** و**الجنس** و**الصورة الشخصية** اختياريًا.
4. اضبط **نوع المستخدم** على **طبيعي**.
5. في **معلومات الحساب**:
   - أدخل **اسم المستخدم** و**البريد الإلكتروني**، ويجب أن يكون كلاهما فريدًا.
   - اضبط **حساب تابع لمنظمة** على **نعم** لموظفي مؤسستك، إذ لا يمكن منح دور في الهيكل التنظيمي إلا للحسابات التابعة للمنظمة.
6. اختر **حفظ**. تؤكد رسالة خضراء حفظ المستخدم، وتوضّح رسالة حمراء البيانات الناقصة أو الخاطئة.

تتلقى لينا رسالة بريد إلكتروني تتضمن رابطًا لتعيين كلمة مرورها. وإن لم تصلها الرسالة، فراجع استكشاف الأخطاء وإصلاحها.

تجهيز المستخدم الجديد كي يبدأ العمل

نفّذ هذه الخطوات لكل شخص جديد، بهذا الترتيب. ويُعدّ تجاوز الخطوة 1 السبب الأكثر شيوعًا لشكوى المستخدم الجديد من أنه «لا يرى شيئًا».

1. **امنحه مستوى صلاحية على النظام لا يقل عن مقيّد.** فالشخص الذي لم يُمنح مستوى صلاحية على النظام يُمنع من الوصول إلى كل شيء تقريبًا، حتى إن أتاحت له مجموعةٌ الوصول إلى شيء ما. وأسهل طريقة هي منح مستوى **مقيّد** مرة واحدة لمجموعة ينتمي إليها الجميع، ليحصل عليه الشخص تلقائيًا في الخطوة 2. راجع امنح الجميع مستوى أساسيًا.
2. **أضِفه إلى مجموعاته.** مثلًا، أضِف لينا إلى مجموعة **الموارد البشرية**. راجع إدارة المجموعات.
3. **امنحه دوره في الهيكل التنظيمي.** مثلًا، *موظف موارد بشرية* في إدارة الموارد البشرية، مع ضبط مستوى الإسناد على **رئيسي**. ويحدّد ذلك أيضًا وحدته التنظيمية ومديره المباشر، اللذين يستند إليهما سير العمل لتوجيه الاعتمادات. راجع إسناد الأشخاص إلى دور.

4. **أضِفه إلى المساحات التي يعمل فيها**، إن كانت مؤسستك تستخدم أكثر من مساحة. راجع المساحات والنطاقات.
5. **تحقق من النتيجة.** افتح **الإدارة › إدارة الوصول › أذونات وصول المستخدم**، واختر الشخص، وتحقق من أن لديه ما يحتاج إليه لأداء عمله. راجع تحقّق مما يستطيع شخص ما الوصول إليه.

البحث عن مستخدم وفتحه

1. افتح **الإدارة › المنظمة › المستخدمون**.
2. ابحث عن الشخص، أو رشّح القائمة. ويمكنك التبديل بين وجه الجدول ووجه البطاقات.
3. اختر صف الشخص لفتح مُدخله.

يعرض المُدخل بيانات الشخص، ومعلومات حسابه، ووحدته التنظيمية، وأدواره، ومديره المباشر. وتعرض القوائم المرتبطة فيه مجموعاته وغيرها من المُدخلات المرتبطة. وتتيح لك منطقة **المناقشة** كتابة ملاحظات للمسؤولين الآخرين والإشارة إليهم باستخدام **@**، ويعرض **السجل التاريخي** كل تغيير أُجري على المُدخل.

تعديل مستخدم

1. في قائمة المستخدمين، اختر النقاط الثلاث (…) في نهاية صف الشخص، ثم اختر **تعديل**.
2. أجرِ التغييرات، ثم اختر **حفظ**.

تسري تغييرات اسم المستخدم وعنوان البريد الإلكتروني فورًا على حساب تسجيل الدخول الخاص بالشخص، ولا يؤدي تعديل المستخدم إلى تغيير كلمة مروره أبدًا. وإذا تركت اسم المستخدم أو البريد الإلكتروني فارغًا، يحتفظ حساب تسجيل الدخول بالقيمة الحالية للحقل.

إعادة تعيين كلمة مرور مستخدم

حين ينسى شخص كلمة مروره ولا يستطيع استخدام **هل نسيت كلمة المرور؟** بنفسه في صفحة تسجيل الدخول:

1. في قائمة المستخدمين، اختر النقاط الثلاث (…) في صف الشخص، ثم اختر **إعادة تعيين كلمة المرور**.
2. أكّد باختيار **إعادة تعيين**.

تظهر لك الرسالة «تم إرسال بريد إلكتروني إلى العنوان المدخل برابط لإعادة تعيين كلمة المرور». يتبع الشخص الرابط ليختار كلمة مرور جديدة، ولا يعمل سوى أحدث رابط.

لا تستخدم هذا الإجراء للأشخاص الذين يسجّلون الدخول عبر الدخول الموحّد أو الذين استُوردوا من دليل شركتك، فليست لديهم كلمة مرور في أسس يمكن إعادة تعيينها؛ إذ تُدار كلمات مرورهم لدى مزوّد الهوية في مؤسستك.

تعطيل حساب أو إعادة تفعيله

عطّل الحساب لمنع شخص من تسجيل الدخول مع الاحتفاظ بكل ما يخصه: مُدخله، وسجله، ومجموعاته، وأدواره. واستخدم هذا الإجراء عند مغادرته، أو غيابه مدة طويلة، أو الاشتباه في اختراق حسابه.

1. في قائمة المستخدمين، اختر النقاط الثلاث (…) في صف الشخص، ثم اختر **تعطيل الحساب**.
2. أكّد باختيار **ايقاف**.

يُسجَّل خروج الشخص فورًا من كل مكان وعلى كل جهاز، ولا يستطيع تسجيل الدخول بأي طريقة. وإذا حاول، تظهر له الرسالة «الحساب معطل، يرجى التواصل مع مسؤول النظام».

وللسماح له بتسجيل الدخول مجددًا، اختر **تفعيل الحساب** من القائمة نفسها، فيتمكّن من تسجيل الدخول بكلمة مروره الحالية.

لا يمكنك تعطيل حسابك أنت.

أرشفة مستخدم واستعادته

أرشِف المستخدم حين ينبغي ألا يبقى الحساب موجودًا إطلاقًا، كحساب مكرر أو تجريبي. فالأرشفة تحذف حساب تسجيل الدخول الخاص بالشخص، بما في ذلك كلمة مروره ومفاتيح مروره وإعدادات المصادقة الثنائية، مع إبقاء مُدخل المستخدم في الأرشيف.

1. في قائمة المستخدمين، اختر النقاط الثلاث (…) في صف الشخص، ثم اختر **أرشفة**.
2. أكّد.

ولاستعادة مستخدم مؤرشف، رشّح قائمة المستخدمين على **مؤرشف**، واختر النقاط الثلاث (…) في الصف، ثم اختر **استعادة مدخل مؤرشف**. يُنشئ أسس عندئذٍ حساب تسجيل دخول جديدًا، ويرسل إلى الشخص بالبريد الإلكتروني رابطًا لتعيين كلمة مرور جديدة، ولا تعود كلمة مروره القديمة تعمل. `Since 1.6`

تعطيل أم أرشفة؟

لمن يغادرون، اختر **التعطيل**؛ فهو فوري وقابل للتراجع، ويُبقي الحساب مرتبطًا بكل ما فعله الشخص. ولا تؤرشف إلا الحسابات التي ما كان ينبغي أن توجد أصلًا.

إنهاء خدمة شخص يغادر

مثال: يغادر عمر الشركة يوم الجمعة. نفّذ ما يلي في آخر يوم عمل له، أو بعده مباشرةً.

1. **عطّل حسابه.** راجع تعطيل حساب أو إعادة تفعيله. سيُسجَّل خروجه فورًا من كل مكان.
2. **سلّم عمله المفتوح لغيره.** تبقى الطلبات التي تنتظر إجراءً من عمر مُسندةً إليه حتى ينقلها أحد. افتح كل طلب منها، ثم افتح **أوامر المدير**، واختر **تغيير المالك**، وحدّد الزميل الذي سيتولّاه.
3. **أنهِ تفويضاته.** افتح أي تفويض يكون فيه عمر هو **المفوض** أو **المفوض له**، واضبط **إلى تاريخ** على تاريخ اليوم، أو اضبط **نشط** على **غير نشط**. راجع التفويض.
4. **أزِله من مجموعاته وأدواره.** فتعطيل الحساب لا يزيله من المجموعات ولا من الهيكل التنظيمي. وإذا كانت مجموعة تملك خطوة في سير العمل، فقد يُختار العضو المعطَّل مالكًا لها، لذا أزِله. راجع إدارة المجموعات وإدارة الأدوار.
5. **أزِل الوصول الممنوح له مباشرةً.** في **الإدارة › إدارة الوصول › أذونات وصول المستخدم**، اختر عمر وأزِل أي أذونات موسومة بـ **إذن مُعطاة مباشرة**.
6. **عيّن مديرًا جديدًا لفريقه.** إذا كان عمر يدير وحدة تنظيمية، فعيّن لها مديرًا جديدًا كي لا تتوقف الاعتمادات. راجع الوحدات التنظيمية.

وإذا كان حساب عمر مستوردًا من دليل شركتك، فتأكد أيضًا من إزالته أو تعطيله هناك، إذ لا يعطّل استيراد الدليل حسابات الأشخاص في أسس عند إزالتهم من الدليل.

مستخدمو التطبيقات

يتيح مستخدم التطبيق لنظام آخر استدعاء أسس باستخدام **رمز API**. ويعامل أسس كل استدعاء على أنه صادر عن مستخدم التطبيق هذا، فتقتصر إمكانات النظام الآخر على ما تمنحه لمستخدم التطبيق من وصول، تمامًا كما هو الحال مع المستخدم البشري.

إضافة مستخدم تطبيق

1. افتح **الإدارة › المنظمة › المستخدمون** واختر **إضافة مستخدم**.
2. في **المعلومات الاساسية**، أدخل اسمًا واضبط **نوع المستخدم** على **تطبيق**.
3. املأ **معلومات الحساب** كما تفعل عند إضافة شخص.
4. في **معلومات التطبيق**، أدخل **الاسم** الخاص بالتطبيق، ثم اختر ألا تنتهي صلاحية الرمز أبدًا، أو أدخل **تاريخ الانتهاء**.
5. اختر **حفظ**.

يُرسل الرمز بالبريد الإلكتروني **إليك** أنت، بصفتك المسؤول الذي أنشأ مستخدم التطبيق، ولا يُعرض على الشاشة أبدًا. سلّمه عبر قناة آمنة إلى الفريق الذي يشغّل النظام الآخر، وامنح مستخدم التطبيق مستوى الصلاحية على النظام والوصول اللذين يحتاج إليهما، كما تفعل مع الشخص.

إعادة إنشاء رمز التطبيق `Since 1.8`

أعِد إنشاء الرمز إذا احتملت تسرّبه، أو حين يوشك على الانتهاء.

1. في قائمة المستخدمين، اختر النقاط الثلاث (…) في صف مستخدم التطبيق، ثم اختر **إعادة إنشاء الرمز**.
2. أكِّد.

يُرسل الرمز الجديد إليك بالبريد الإلكتروني، ويظل الرمز القديم يعمل خلال فترة سماح قصيرة لإتاحة الوقت للنظام الآخر للانتقال إلى الرمز الجديد. ويحتفظ التطبيق بهويته ووصوله وسجله. ولا يمكنك إعادة إنشاء رمز مستخدم تطبيق مؤرشف، لكن يمكنك ذلك لمستخدم تطبيق معطَّل.

انتهاء صلاحية الرمز `Since 1.10`

يظهر **تاريخ الانتهاء** لمستخدم التطبيق في النموذج، ويمكن تعديله ما لم يكن الرمز مضبوطًا على عدم الانتهاء. ويتوقف الرمز عن العمل بعد ذلك التاريخ. وهذا التاريخ اختياري: اتركه فارغًا، أو اختر عدم الانتهاء، للحصول على رمز لا تنتهي صلاحيته.

وإذا توقف رمز مستخدم تطبيق عن العمل بعد الترقية إلى 1.10، فافتح مستخدم التطبيق، وأدخل **تاريخ الانتهاء** مجددًا، ثم احفظ.

للتعمّق أكثر

لمطوّري التكامل: رموز الـ API [التكامل والتوسعة › استخدم رمز API] · واجهة المستخدمين البرمجية وحسابات الهوية [التكامل والتوسعة]

معلومات مفيدة

- **كلمات المرور** يجب ألا تقل عن 8 أحرف، وأن تتضمن أحرفًا كبيرة وصغيرة ورقمًا ورمزًا. وعندما يغيّر المستخدمون كلمات مرورهم، يجب ألا تطابق كلمة المرور الجديدة القديمة.
- **الحسابات المقفلة.** بعد 5 محاولات متتالية بكلمة مرور خاطئة، يُقفل الحساب بضع دقائق، وتطول مدة القفل إذا تكرر ذلك. وتظهر للمستخدمين الرسالة «الحساب مقفل». ولا يوجد زر لفك القفل، إذ ينتهي القفل تلقائيًا، ويزيله تسجيل الدخول الناجح.
- **أسماء المستخدمين وعناوين البريد الإلكتروني لا تميّز بين الأحرف الكبيرة والصغيرة.** فـ `Lina@example.com` و`lina@example.com` عنوان واحد.
- **إعدادات المصادقة الثنائية، ومفاتيح المرور، والتفضيلات الشخصية** (اللغة، والسمة، والمنطقة الزمنية، وصيغة التاريخ) تخص الشخص نفسه، ويديرها من صفحتَي **الأمان** و**تفضيلات المستخدم** الخاصتين به. راجع أمان الحساب [استخدام أسس › أمان الحساب وكشف القيم المحمية].
- **إضافة حقول إلى المستخدمين.** كيان المستخدمين كيان بيانات كغيره، لذا يستطيع باني التطبيقات أن يضيف إليه حقولًا ومعارض وعلاقات. راجع نمذجة البيانات: الكيانات [بناء التطبيقات › إنشاء كيان وتصميمه].

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
لم تصل رسالة تعيين كلمة المرور إلى مستخدم جديد.	تحقق من عنوان البريد الإلكتروني في المُدخل؛ فإذا كان حساب آخر يستخدم ذلك العنوان، فلن يُنشأ حساب تسجيل دخول للمستخدم الجديد؛ غيّر أحد العنوانين. وتحقق أيضًا من سجل البريد الإلكتروني في **الإدارة › المراقبة › السجلات**، ثم استخدم **إعادة تعيين كلمة المرور** لإرسال رابط جديد.
مستخدم جديد يسجّل الدخول لكنه لا يرى شيئًا.	ليس لديه مستوى صلاحية على النظام. امنحه مستوى **مقيّد** على الأقل، ويكون ذلك عادةً عبر مجموعة. راجع الخطوة 1.
تظهر الرسالة «User must be an organization account» حين تُسند دورًا.	اضبط **حساب تابع لمنظمة** على **نعم** في مُدخل المستخدم، ثم أسنِد الدور مجددًا.
يطلب مستخدم يسجّل الدخول عبر الدخول الموحّد أو من الدليل إعادة تعيين كلمة المرور.	ليست لديه كلمة مرور في أسس. وجّهه إلى المسؤول عن إدارة مزوّد الهوية في شركتك.
لا يظهر **تعطيل الحساب**.	فتحت الصف الخاص بك، أو أن الحساب معطّل بالفعل (ابحث عن **تفعيل الحساب**).
توقف رمز مستخدم تطبيق عن العمل.	تحقق من **تاريخ الانتهاء** الخاص به، ومما إذا كان مستخدم التطبيق قد عُطّل أو أُعيد إنشاء رمزه.

ⓘ للتعمّق أكثر

لمطوّري التكامل: واجهة المستخدمين البرمجية وحسابات الهوية [التكامل والتوسعة] · للمشغّلين: خادم الهوية ·
للمستخدمين النهائيين: أمان الحساب [استخدام أسس › أمان الحساب وكشف القيم المحمية]

إدارة المجموعات

هذا الدليل موجّه إلى مسؤولي القاطن. تتيح لك المجموعة التعامل مع فريق كامل بوصفه وحدة واحدة؛ فتمنح المجموعةَ الأذونات، وتُسند إليها العمل، وترسل إليها الإشعارات، ليحصل كل عضو فيها على ذلك. ستتعلّم هنا أيّ أنواع المجموعات تختار، وكيف تنشئ مجموعة وتضيف إليها الأعضاء وتدير عضويتها.

المثال المستخدم هو مجموعة **الموارد البشرية** التي تضم جميع العاملين في إدارة الموارد البشرية.

كيف تعمل

بدلًا من منح كل شخص الأذونات نفسها واحدًا تلو الآخر، امنحها مرة واحدة لمجموعة، فيحصل عليها كل من فيها. وحين ينضم أحد إلى الفريق أو يغادره، يكفيك تحديث العضوية. ويحصل الشخص على أعلى مستوى وصول تمنحه أذوناته الفردية وأذونات جميع المجموعات التي ينتمي إليها.

وتُستخدم المجموعات أيضًا خارج نطاق الأذونات؛ إذ يستطيع باني التطبيقات أن يجعل مجموعةً مالكةً لخطوة في سير العمل، أو مستلمةً لإشعار، أو جمهورًا لتعليق، فيحدّد أسس أعضاء المجموعة في تلك اللحظة.

أنواع المجموعات

تعرض قائمة **المجموعات** جميع أنواع المجموعات في مكان واحد. ويمكنك بنفسك إنشاء **مجموعات المستخدمين** و**مجموعات الاستعلام** وتعديلها فقط، أما الأنواع الأخرى فتُدار عضويتها تلقائيًا.

النوع	من فيها	كيف تديرها
مجموعة مستخدمين	الأشخاص الذين تضيفهم.	**الإدارة › المنظمة › مجموعات المستخدمين**. وهذا هو النوع المعتاد.
مجموعة استعلام	كل مستخدم يطابق استعلامًا محفوظًا، مثل «كل من يتضمن مسمّاه الوظيفي كلمة مدير». وينضم الأشخاص إليها ويغادرونها تلقائيًا كلما تغيّرت بياناتهم.	**الإدارة › المنظمة › مجموعات الاستعلام**.
مجموعة دور	كل من يشغل دورًا ما، مثل *مدير الموارد البشرية*، ولكل دور مجموعة.	أسنِد الأشخاص إلى الدور. راجع إدارة الأدوار.
مجموعة وحدة تنظيمية	كل من أُسنِد إلى وحدة من وحدات الهيكل التنظيمي، ولكل وحدة مجموعة.	أسنِد الأشخاص إلى الوحدة. راجع الوحدات التنظيمية.

ويحتفظ النظام كذلك ببضع مجموعات داخلية خاصة به، لا يمكنك إنشاؤها أو تغييرها.

إدارة ما: مجموعة أم دور أم وحدة تنظيمية أم مجموعة استعلام؟

مثال: تريد أن تطّلع «إدارة الموارد البشرية» على تقارير الموارد البشرية وأن تتلقى إشعاراتها.

- **هل إدارة الموارد البشرية وحدةٌ في هيكلك التنظيمي أصلًا؟** استخدم **مجموعة وحدة تنظيمية** التابعة لها؛ إذ تتبع عضويتها الهيكل التنظيمي، فتديرها في مكان واحد.
- **هل هي منصب لا فريق** (كل *مدير موارد بشرية* أيًّا كان موقعه)؟ استخدم **مجموعة دور**.
- **هل تتجاوز حدود الهيكل التنظيمي** (لجنة موارد بشرية تضم أشخاصًا من عدة إدارات)؟ أنشئ **مجموعة مستخدمين** وأضِف إليها الأشخاص.

- **هل يمكن وصفها بقاعدة** (كل من كانت قيمة حقل الإدارة لديه *الموارد البشرية*)؟ أنشئ **مجموعة استعلام** كي لا يضطر أحد إلى تحديث القائمة يدويًا.
- **هل يأتي الأشخاص من دليل شركتك؟** استخدم **مجموعة مستخدمين** تُضاف عضويتها من الدليل. راجع المستخدمون من دليل شركتك.

تضم المجموعة *أشخاصًا*، فلا تخلط بينها وبين **القائمة** التي تضم مُدخلات أو قيمًا. راجع التجميعات والقوائم [استخدام أسس › القوائم: اجمع المُدخلات معًا].

قبل أن تبدأ

- تحتاج إلى مستوى **إدارة** على النظام كي ترى قائمة **المنظمة**.
- يجب أن يكون الأشخاص الذين تريد إضافتهم موجودين مسبقًا بوصفهم مستخدمين. راجع إدارة المستخدمين.

إنشاء مجموعة

1. افتح **الإدارة › المنظمة › مجموعات المستخدمين**.
2. اختر **إضافة مجموعة المستخدمين**.
3. أدخل **اسم المجموعة** (مثل *الموارد البشرية*)، ويمكنك اختياريًا إدخال **وصف المجموعة** و**أيقونة المجموعة**.
4. اختر **حفظ**.

ثم أضِف الأعضاء كما هو موضح أدناه.

إضافة الأعضاء أو إزالتهم

1. افتح **الإدارة › المنظمة › مجموعات المستخدمين**، ثم افتح المجموعة.
2. افتح تبويب **المستخدمين** الخاص بالمجموعة.
3. أضِف الأشخاص الذين ينتمون إلى المجموعة، أو أزِل من غادرها.

ويمكنك أيضًا إدارة العضوية من صفحة الشخص: افتح المستخدم من **الإدارة › المنظمة › المستخدمون**، واستخدم تبويب **المجموعات** الخاص به.

لا يُدرَج الشخص في المجموعة إلا مرة واحدة مهما تكررت إضافته، ولا تُحتسب العضوية إلا للمستخدمين النشطين؛ إذ يخرج المستخدم المؤرشف من جميع المجموعات تلقائيًا.

إنشاء مجموعة استعلام

تحتاج مجموعة الاستعلام إلى استعلام محفوظ على كيان **المستخدمون** يختار الأشخاص المطلوبين. فإن لم يكن موجودًا بعد، فاطلب من أحد بُناة التطبيقات إنشاءه. راجع الاستعلامات [بناء التطبيقات › الاستعلامات والمرشّحات].

1. افتح **الإدارة › المنظمة › مجموعات الاستعلام**.
2. اختر **إضافة مجموعة استعلام المستخدمين**.
3. أدخل **اسم المجموعة**، ويمكنك اختياريًا إدخال **التوصيف** و**أيقونة**.
4. في **الاستعلام**، اختر الاستعلام المحفوظ.

5. اختر **حفظ**.

يضيف أسس أعضاء المجموعة وفق الاستعلام، ويُحدّث عضويتها كلما تغيّرت بيانات الأشخاص، فلا حاجة إلى إضافة الأعضاء أو إزالتهم يدويًا.

البحث عن المجموعات واستعراضها

- **كل أنواع المجموعات:** افتح **الإدارة › المنظمة › المجموعات**، ويبيّن لك عمود **نمط المجموعة** نوع كل منها.
- **المجموعات التي أنشأتها فقط:** افتح **مجموعات المستخدمين** أو **مجموعات الاستعلام**.

اختر مجموعة لعرض تفاصيلها. ويمكنك في كل قائمة البحث بالاسم، والتبديل بين وجه الجدول ووجه البطاقات، والفرز، والترشيح حسب الحالة لإظهار المجموعات المؤرشفة مثلًا.

ويستطيع غير المسؤولين رؤية المجموعات المرتبطة بحساباتهم وأدوارهم إذا أتحت لهم أنت أو أحد بُناة التطبيقات معرضًا يعرضها.

تعديل مجموعة أو أرشفتها

التعديل. في **مجموعات المستخدمين** (أو **مجموعات الاستعلام**)، اختر النقاط الثلاث (…) في نهاية صف المجموعة، ثم اختر **تعديل**، وأجرِ تغييراتك، ثم اختر **حفظ**.

الأرشفة. اختر النقاط الثلاث (…) في صف المجموعة، ثم اختر **أرشفة**، وأكّد ذلك.

قبل أرشفة مجموعة، تحقّق من مواضع استخدامها الحالية: أذوناتها (**الإدارة › إدارة الوصول › أذونات وصول المجموعة**)، وأي خطوة في سير العمل أو إشعار وجّهه أحد بُناة التطبيقات إليها، ووجّه كل ذلك إلى مجموعة أخرى أولًا.

لا يمكن تعديل مجموعات الأدوار ومجموعات الوحدات التنظيمية أو أرشفتها؛ فهي تتغيّر بتغيير الدور أو الوحدة.

منح مجموعة أذونات

امنح المجموعة الأذونات من شاشات **إدارة الوصول**. راجع الأذونات والوصول، ولمثال تطبيقي راجع اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط.

معلومات مفيدة

حين تتولى مجموعة خطوة في سير العمل

إذا جعل باني التطبيقات مجموعةً مالكةً لخطوة في سير العمل، تُسنَد الخطوة عادةً إلى عضو **واحد** من المجموعة، لا إلى جميع أعضائها. وما لم يختر الباني غير ذلك، تُسنَد إلى العضو الأول وفق ترتيب الأعضاء في المجموعة. ويستطيع الباني بدلًا من ذلك إسناد الخطوة إلى مدير الوحدة التنظيمية للمجموعة، أو إتاحة اختيار المالك يدويًا لأحد الأشخاص، أو إسنادها إلى جميع الأعضاء بالتوازي. فإذا استمر إسناد العمل إلى الشخص نفسه، فاسأل الباني عن طريقة إعداد الخطوة. راجع سير العمل [بناء التطبيقات › سير العمل والاعتمادات].

ولهذا السبب، أزِل المغادرين من مجموعاتهم فورًا، حتى بعد تعطيل حساباتهم. راجع إنهاء خدمة شخص يغادر.

المجموعات لا تنتقل ضمن الحزم

المجموعات وأعضاؤها من المستخدمين خاصة بكل بيئة. فحين ينقل باني التطبيقات تطبيقًا من بيئة الاختبار إلى بيئة الإنتاج ضمن حزمة، يحتفظ سير العمل والمعارض بالإشارات إلى المجموعات، لكن المجموعات نفسها وأعضاءها لا تُنسخ. لذا تأكّد قبل تثبيت الحزمة من وجود مجموعة بالاسم نفسه في البيئة الهدف تضم الأشخاص المناسبين.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
عضو في المجموعة لا يحصل على أذونات المجموعة.	ربما لا يملك الشخص أي مستوى صلاحية على النظام إطلاقًا. امنحه **مقيّد** على الأقل. راجع امنح الجميع مستوى أساسيًا.
شخص غير موجود في مجموعة استعلام.	بياناته لا تطابق الاستعلام. افتح مُدخل المستخدم الخاص به وقارنه بشروط الاستعلام.
لا يمكنك تعديل مجموعة أو أرشفتها.	إنها مجموعة دور أو مجموعة وحدة تنظيمية. غيّر الدور أو الوحدة التنظيمية بدلًا من ذلك.
بعد تثبيت حزمة، تشير خطوة أو معرض إلى مجموعة غير موجودة.	أنشئ المجموعة في هذه البيئة، أو اطلب من الباني توجيه الخطوة أو المعرض إلى مجموعة موجودة.

للتعمّق أكثر

لمطوّري التكامل: المجموعات والوحدات التنظيمية والعضوية [التكامل والتوسعة › المجموعات والوحدات التنظيمية والانتماء] ·
لبُناة التطبيقات: سير العمل: مالكو الخطوات [بناء التطبيقات › سير العمل والاعتمادات]

إدارة الأدوار

هذا الدليل موجّه إلى مسؤولي القاطن: إذ تتعرّف فيه إلى الغرض من الأدوار، وكيف تنشئها وتعدّلها، وكيف تُسند الأشخاص إلى دور، وكيف تمنح كل من يشغل الدور الوصول نفسه في خطوة واحدة. وتستخدم الأمثلة دور **مدير الموارد البشرية** في قسم الموارد البشرية.

الغرض من الأدوار

يصف الدور منصبًا أو مسؤولية، مثل *مدير الموارد البشرية* و*مسؤول الرواتب* و*رئيس القسم*، ويفيدك في ثلاثة جوانب:

- **الوصول.** امنح الدور الوصول مرة واحدة، فيحصل عليه كل من أُسند إليه؛ وحين ينضمّ شخص إلى الدور أو يغادره، يتغيّر وصوله تلقائيًا تبعًا لذلك.
- **سير العمل.** يمكن أن يكون الدور مالكًا لخطوة في سير العمل، فيصل الطلب إلى من يشغل ذلك الدور حاليًا.
- **التنظيم.** تُسنَد الأدوار ضمن هيكلك التنظيمي، فتعرف المنصة من يشغل كل منصب، والوحدة التي يشغله فيها، ومن يدير كل وحدة.

ولكل دور مجموعة تضمّ دائمًا الأشخاص المُسنَدين إليه، وهي المجموعة التي تختارها حين تمنح الدور وصولًا.

> **معنيان لكلمة «الدور»**
>
> الأدوار في هذه الصفحة هي التي تنشئها أنت وتسمّيها، وتختلف عن **مستوى النظام** للشخص (مقيّد، عرض، مطور، تعديل، إدارة)، الذي تضبطه من **الإدارة › إدارة الوصول › أذونات المدير**. راجع الأذونات والوصول.

اعثر على قائمة الأدوار

افتح **الإدارة › المنظمة › الأدوار**.

تعرض القائمة اسم كل دور ووصفه، وطريقة ارتباطه بالهيكل التنظيمي، ونوعه، ونوع إسناده؛ كما يمكنك ترتيب القائمة والبحث فيها وترشيحها، والتبديل بين طرق العرض: الجدول والبطاقات واللوحة.

أنشئ دورًا

1. افتح **الإدارة › المنظمة › الأدوار**.
2. اختر زر الإضافة أعلى القائمة.
3. املأ النموذج:

- **اسم الدور** – مثل *مدير الموارد البشرية*.
- **وصف الدور** – اختياري: اذكر فيه مسؤوليات الدور.
- **الارتباط بالهيكلية** – أين يمكن شغل الدور:

- **غير مرتبط بالهيكلية** – الدور غير مرتبط بموضع في هيكلك التنظيمي، مثل *مسؤول السلامة من الحرائق*.
- **مرتبط بوحدة تنظيمية واحدة** – الدور موجود في وحدة واحدة، مثل *مدير الموارد البشرية* في قسم الموارد البشرية.
- **مرتبط بعدة وحدات تنظيمية** – الدور نفسه موجود في عدة وحدات، مثل *سكرتير القسم*.

- **نوع الدور**:
  - **موقع وظيفي** – منصب فعلي في الهيكل التنظيمي.
  - **دور مجرد** – مسؤولية يتولّاها الشخص إلى جانب منصبه.

لا يمكن أن يكون الدور غير المرتبط بأي وحدة تنظيمية موقعًا وظيفيًا.

- **نوع الإسناد**:
  - **فريد** – لا يشغل الدور إلا شخص واحد في الوقت نفسه، مثل *مدير الموارد البشرية*.
  - **متكرر** – يمكن أن يشغله أشخاص عدة، مثل *موظف الموارد البشرية*.

4. اختر **حفظ**؛ إذ تؤكّد رسالة خضراء نجاح الحفظ، وتخبرك رسالة حمراء بما يلزم إصلاحه.

اعرض الدور أو عدّله أو أرشِفه

الاطّلاع. افتح الدور من القائمة؛ إذ يعرض تبويب **التفاصيل** تفاصيل الدور، ويتيح تبويب **المناقشة** للأشخاص التعليق وإرفاق الملفات (وتُضبط أنواع الملفات المسموح بها وحجمها – نحو 1 ميغابايت افتراضيًا – لكل معرض على حدة)، بينما يسجّل تبويب **التاريخ** كل تغيير.

التعديل.

1. في قائمة الأدوار، اختر النقاط الثلاث (…) في نهاية صف الدور، ثم اختر **تعديل**.
2. غيّر التفاصيل، ثم اختر **حفظ**.

الأرشفة. أرشِف الدور الذي لم تعد بحاجة إليه.

1. في قائمة الأدوار، اختر النقاط الثلاث (…) في نهاية صف الدور، ثم اختر **أرشفة**.
2. أكّد باختيار **أرشفة**.

لا يمكن إسناد الدور المؤرشف بعد ذلك، لذا تحقّق قبل أرشفته من أن أحدًا لم يعد يحتاج إليه.

أسند الأشخاص إلى دور

يُشغَل الدور دائمًا ضمن وحدة في الهيكل التنظيمي، لذا يحدّد كل إسناد الشخص والدور والوحدة. والإسنادات مُدخلات في كيان البيانات **الإسناد**؛ أما صفحة **الهيكل التنظيمي** فتسرد وحداتك، لكنها لا تبيّن من يشغل أيّ دور.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح **الإسناد** واختر زر الإضافة، فيُفتح نموذج إسناد جديد.
2. املأ الحقول:

- **الدور** – مثل *مدير الموارد البشرية*.
- **مستوى الإسناد** – **رئيسي** للدور الأساسي للشخص، أو **إضافي** لدور يشغله إلى جانبه.
- **نوع الإسناد** – **أصيل** للإسناد العادي، أو **تفويض** حين يتولّى الشخص الدور نيابةً عن غيره.
- **المستخدم** – الشخص المعنيّ.
- **الوحدة التنظيمية** – الوحدة، مثل قسم الموارد البشرية.
- **مدير** – فعّله إذا كان هذا الشخص يدير الوحدة.

3. احفظ.

تتحقّق المنصة من كل إسناد قبل حفظه؛ فهي ترفض مثلًا إسناد شخص ثانٍ إلى دور **فريد**، وحين تتغيّر الإسنادات، يُحدَّث مدير الوحدة تلقائيًا. ولمزيد من التفاصيل عن الوحدات ومديريها، راجع الوحدات التنظيمية.

امنح دورًا وصولًا

امنح الدور الوصول تمامًا كما تمنحه لأي مجموعة: اختر مجموعة الدور حيثما تطلب منك الشاشة اختيار مجموعة.

مثال: اسمح لكل مدير موارد بشرية بفتح تقرير «عدد الموظفين حسب القسم».

1. افتح **الإدارة › إدارة الوصول › أذونات وصول المجموعة**.
2. في **اختر المجموعة**، اختر مجموعة دور **مدير الموارد البشرية**.
3. اختر **إضافة إذن**، ثم اختر التقرير في **الكائن**، واحفظ.

يحصل الشخص على أعلى مستوى وصول تمنحه إياه منحه كلها: منحه المباشرة، ومنح مجموعاته، ومنح أدواره. وللاطلاع على مستويات الوصول، وكيف تتراكم المنح، ومزيد من المهام، راجع الأذونات والوصول.

خصّص كيان الأدوار

الأدوار كيان بيانات كغيره، لذا يستطيع باني التطبيقات أن يضيف إليه حقولًا ومعارض وعلاقات، مثل حقل *الدرجة الوظيفية*، ويتبع ذلك الخطوات نفسها المتّبعة مع أي كيان آخر؛ راجع نمذجة البيانات: الكيانات [بناء التطبيقات › إنشاء كيان وتصميمه].

استكشاف الأخطاء وإصلاحها

لا أستطيع إسناد شخص ثانٍ إلى الدور. نوع الإسناد في هذا الدور هو **فريد**؛ لذا غيّره إلى **متكرر** إذا كان ينبغي أن يشغله أكثر من شخص.

لا يمكن حفظ الدور بوصفه موقعًا وظيفيًا. يجب أن يرتبط الموقع الوظيفي بوحدة تنظيمية واحدة على الأقل؛ فغيّر **الارتباط بالهيكلية**، أو اختر **دور مجرد**.

شخص مُسنَد إلى الدور لا يملك وصول الدور. تحقّق من أن الإسناد محفوظ وساري المفعول، ثم ابحث عن الشخص في **الإدارة › إدارة الوصول › أذونات وصول المستخدم**؛ إذ يبيّن لك **مكتسبة عن طريق** الأدوارَ والمجموعات التي تمنحه كل إذن.

للتعمّق أكثر

لمطوّري التكامل: واجهة برمجة الأذونات – نموذج بيانات الأدوار [التكامل والتوسعة › واجهة الأذونات البرمجية] · لمهندسي المنصة: المحرّك: الأذونات والمصوّتون

الوحدات التنظيمية

هذا الدليل موجّه إلى مسؤولي القاطن، ويوضّح لك كيف تبني هيكل مؤسستك، أي **الهيكل التنظيمي**، في أسس: تنشئ الوحدات، وترتّبها بعضها تحت بعض، وتسند الأشخاص إليها، وتختار من يدير كلًّا منها. ويعتمد سير العمل والإشعارات على هذا الهيكل لتحديد المدير المناسب؛ فإذا كان الهيكل التنظيمي صحيحًا، وصلت الاعتمادات إلى الشخص الصحيح دون أن يختاره أحد يدويًا.

يعتمد المثال على شركة متوسطة الحجم: **الإدارة التنفيذية** في القمة، وتحتها إدارة **الموارد البشرية**، وتحت الموارد البشرية قسم **التوظيف**.

كيف تعمل

الوحدة التنظيمية موضع واحد في هيكلك التنظيمي: مديرية، أو إدارة، أو قسم، أو فريق. ولكل وحدة **أب**، أي الوحدة التي تندرج تحتها، وبذلك تشكّل الوحدات شجرة تتصدّرها وحدة واحدة.

ويُسند الأشخاص إلى الوحدات عبر **الإسنادات**؛ فالإسناد يعني «هذا الشخص يشغل هذا الدور في هذه الوحدة». مثال: *لينا* هي *موظفة موارد بشرية* في *التوظيف*. ولكل شخص إسناد **رئيسي** واحد يحدّد وحدته الأساسية، ويمكن أن تكون له إسنادات **إضافية** إلى جانبه. ويمكن للإسناد أيضًا أن يجعل الشخص **المدير** المسؤول عن الوحدة.

يتحكم الهيكل التنظيمي في ثلاثة أمور:

الأمر	كيف يُستخدم الهيكل التنظيمي
المدير المباشر للشخص	يبدأ أسس من الوحدة الأساسية للشخص ويصعد في الشجرة حتى يصل إلى أقرب وحدة لها مدير غير الشخص نفسه.
الاعتمادات الموجّهة «إلى المدير»	يستطيع باني التطبيقات توجيه خطوة في سير العمل إلى مدير مقدّم الطلب، أو إلى المدير الذي يعلوه بمستويين أو أكثر، فيحدّد أسس ذلك الشخص في الهيكل التنظيمي. ويمكن كذلك إرسال الإشعارات إلى مدير مالك الخطوة.
«الأشخاص القريبون مني»	تعرض بعض حقول اختيار الأشخاص من ينتمون إلى وحدتك، ووحدتها الأب، وجميع الوحدات التي تندرج تحت وحدتك.

مثال. الوحدة الأساسية للينا هي *التوظيف*، وليس لها مدير خاص بها. أما وحدتها الأب، *الموارد البشرية*، فتديرها سارة. لذا تكون سارة المديرة المباشرة للينا، ويذهب طلب الإجازة الموجّه «إلى المدير المباشر» إلى سارة.

> ⓘ **الوحدات التنظيمية والعلامة التجارية لمؤسستك**
>
> تختلف إعدادات **المنظمة** التي تتضمّن اسمك وشعارك وترويستك وتذييلتك عن الوحدات التنظيمية؛ فهي تمنح المنصة هوية مؤسستك ولا تدخل ضمن الهيكل التنظيمي. راجع إعدادات المنظمة.

قبل أن تبدأ

- تحتاج إلى مستوى **إدارة** على النظام لتتمكن من رؤية قائمة **المنظمة**. ولا يستطيع تغيير الهيكل التنظيمي إلا المسؤولون، أما غيرهم فيقتصر دورهم على استعراضه.
- أنشئ أولًا **الأدوار** التي ستُسند الأشخاص إليها، مثل *موظف موارد بشرية* و*مدير الموارد البشرية*. راجع إدارة الأدوار.
- يتضمّن التثبيت الجديد وحدة واحدة في القمة هي **الإدارة التنفيذية**. ابنِ بقية الهيكل تحتها، أو غيّر اسمها.

تخطيط المستويات

المستويات تسميات تبيّن عمق الوحدة في الهيكل: *مديرية*، *إدارة*، *قسم*. وهي تساعد الأشخاص على فهم الهيكل وترشيحه، لكنها لا تغيّر طريقة عمل الشجرة؛ إذ يحدّدها **الأب** وحده.

يحتوي التثبيت الجديد على مستوى واحد هو **المستوى الاول**. ولإضافة المزيد، افتح **الإدارة › التطبيقات › القوائم**، ثم افتح **مستويات الوحدات التنظيمية**، وأضِف المستويات التي تحتاج إليها.

إنشاء وحدة

مثال: إنشاء إدارة الموارد البشرية تحت الإدارة التنفيذية.

1. افتح **الإدارة › المنظمة › الهيكل التنظيمي**.
2. اختر **إضافة وحدة تنظيمية**.
3. أدخل **الاسم** بكل لغة، مثل *الموارد البشرية*. ويجب أن تكون الأسماء فريدة، فلا يجوز أن تحمل وحدتان الاسم نفسه.
4. أضِف **التوصيف** و**الأيقونة** إن شئت.
5. في **الأب**، اختر الوحدة التي تندرج تحتها: *الإدارة التنفيذية*. ولا تترك **الأب** فارغًا إلا للوحدة التي في القمة.
6. في **مستوى الوحدة التنظيمية**، اختر المستوى، مثل *إدارة*.
7. لا تفعّل **مستوى الإسناد رئيسي** إلا إذا كان مسموحًا للأشخاص في هذه الوحدة بإسنادهم **الرئيسي** فقط، دون أي إسناد **إضافي**.
8. اختر **حفظ**.

كرّر ذلك لكل وحدة، بدءًا من القمة ونزولًا؛ إذ يجب أن تكون الوحدة الأب موجودة قبل أن تتمكن من اختيارها.

ولنقل وحدة، مع كل ما تحتها، إلى جزء آخر من الهيكل، عدّل الوحدة وغيّر **الأب** الخاص بها. ويرفض أسس اختيار أي أب يجعل الوحدة تندرج تحت نفسها أو تحت إحدى وحداتها الفرعية.

وضع الأشخاص في الوحدات

لإضافة شخص إلى وحدة، أسند إليه دورًا فيها.

1. افتح **الإدارة › المنظمة › الهيكل التنظيمي**، ثم افتح الوحدة.
2. أضِف إسنادًا، واملأ ما يلي:
   - **الدور**: مثل *موظف موارد بشرية*.
   - **مستوى الإسناد**: **رئيسي** للوحدة الأساسية للشخص، و**إضافي** لأي دور آخر يشغله.
   - **نوع الإسناد**: **أصيل** للإسناد العادي، أو **تفويض** حين يتولى الشخص الدور نيابةً عن غيره.
   - **المستخدم**: الشخص المعني.
   - **مدير**: فعّله إذا كان هذا الشخص يدير الوحدة.
3. احفظ.

امنح كل شخص إسنادًا **رئيسيًا واحدًا** فقط؛ إذ يرفض أسس إضافة إسناد رئيسي ثانٍ، ويجب أن يكون دور الإسناد الرئيسي من نوع **موقع وظيفي** لا **دور مجرد**. وعندئذ يعرض لك مُدخل المستخدم **الوحدة التنظيمية** و**الدور ذو الإسناد الرئيسي** و**المدير المباشر** الخاصة به. وتجد التفاصيل الكاملة، بما فيها قواعد الأدوار الفريدة، في إسناد الأشخاص إلى دور.

لا يمكن إسناد الأدوار إلا إلى المستخدمين الذين تكون قيمة **حساب تابع لمنظمة** لديهم **نعم**. راجع إضافة مستخدم.

تعيين مدير

مدير الوحدة هو الشخص الذي لديه إسناد **رئيسي** في الوحدة مع تفعيل **مدير**.

- **لاختيار مدير:** أضِف الإسناد الرئيسي لذلك الشخص في الوحدة أو عدّله، وفعّل **مدير**.
- **لتغيير المدير:** ألغِ تفعيل **مدير** في إسناد المدير السابق، وفعّله في إسناد المدير الجديد.

ويُحدَّث حقل **المدير** الخاص بالوحدة تلقائيًا استنادًا إلى الإسنادات، فلا تضبطه يدويًا أبدًا.

ولا يلزم أن يكون للوحدة مدير؛ فالأشخاص في وحدة بلا مدير يتبعون أقرب مدير يعلوهم في الهيكل.

معلومات مفيدة

- **تحقق من الاعتمادات بعد تغيير الهيكل.** ربما أعدّ باني التطبيقات خطوةً لتُوجَّه «مستويين إلى الأعلى». فإذا كان عدد المديرين فوق مقدّم الطلب في الهيكل أقل من ذلك، تبقى الخطوة بلا مالك. وبعد أي إعادة هيكلة، اختبر طلبًا من شخص في كل وحدة تغيّرت.
- **عندما يغادر مدير**، عيّن مديرًا جديدًا لوحدته فورًا، وإلا انتقلت الاعتمادات صعودًا إلى المدير التالي فوقه. راجع إنهاء خدمة شخص يغادر.
- **لكل وحدة مجموعة.** ينضم كل شخص يُسند إلى وحدة تلقائيًا إلى مجموعة الوحدة التنظيمية الخاصة بها، ويمكنك استخدام هذه المجموعة في الأذونات والإشعارات. راجع إدارة المجموعات.
- **إضافة حقول.** يمكن لباني التطبيقات توسيع كيان الوحدة التنظيمية كأي كيان آخر، بإضافة رمز مركز التكلفة مثلًا. راجع نمذجة البيانات: الكيانات [بناء التطبيقات › إنشاء كيان وتصميمه].

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
«User must be an organization account» عند إضافة إسناد.	اضبط **حساب تابع لمنظمة** على **نعم** في مُدخل المستخدم.
لا يمكنك إضافة إسناد رئيسي ثانٍ لشخص ما.	لكل شخص وحدة أساسية واحدة. اختر **إضافي** للإسناد الآخر، أو غيّر إسناده الرئيسي الحالي.
«role must be of type job position if the the assignment level is main»	الدور من نوع **دور مجرد**. استخدمه في إسناد **إضافي**، أو اختر دورًا من نوع موقع وظيفي للإسناد الرئيسي.
لا يمكنك إضافة إسناد **إضافي** في وحدة ما.	خيار **مستوى الإسناد رئيسي** مفعّل في الوحدة.
لا يمكن حفظ وحدة باسم معيّن.	توجد وحدة أخرى تحمل ذلك الاسم بالفعل.
وُجِّه طلب إلى المدير الخطأ، أو لم يُوجَّه إلى أحد.	تحقق من الإسناد الرئيسي لمقدّم الطلب واصعد في الهيكل؛ فأول وحدة فوقه لها مدير هي وجهة الطلب.

للتعمّق أكثر

لمطوّري التكامل: المجموعات والوحدات التنظيمية والانتماء [التكامل والتوسعة] · لبُناة التطبيقات: سير العمل [بناء التطبيقات › سير العمل والاعتمادات]

الأذونات والوصول

يُوجَّه هذا الدليل إلى مسؤولي القاطن، إذ يشرح آلية عمل الوصول في أسس، وأين تُديره في **الإدارة**، وكيفية منح كل شخص الأذونات التي يتطلّبها عمله دون زيادة. وتستند الأمثلة الواردة فيه إلى قسم الموارد البشرية في شركة متوسطة الحجم: مجموعة **الموارد البشرية**، ودور **مدير الموارد البشرية**، وخدمات الموارد البشرية مثل طلبات الإجازة.

كيف يعمل الوصول

يجيب كل إذن عن ثلاثة أسئلة:

- **من** يحصل على الوصول: مستخدم، أو مجموعة، أو دور، أو وحدة تنظيمية.
- **على ماذا**: المنصة كلّها، أو وحدة، أو كيان بيانات، أو معرض أو صفحة أو تقرير أو خدمة بعينها.
- **بأي قدر**: مستوى الوصول، وهو «مقيّد» أو «عرض» أو «مطور» أو «تعديل» أو «إدارة».

ويجمع وصول الشخص كل ما مُنح له مباشرةً وكل ما مُنح لكل مجموعة ودور ووحدة تنظيمية ينتمي إليها.

لمن يمكنك منح الوصول

تمنح الوصول لـ	استخدمه عندما
مستخدم	يحتاج شخص واحد إلى ما لا يحتاجه غيره في فريقه. استخدم هذا الخيار باعتدال، إذ تصعب مراجعته لاحقًا.
مجموعة	يحتاج فريق كامل إلى الوصول نفسه، مثل مجموعة الموارد البشرية؛ وهذا هو الخيار المعتاد.
دور	يحتاجه كل من يشغل منصبًا بعينه، مثل كل مدير موارد بشرية؛ ولكل دور مجموعة تضمّ دائمًا الأشخاص المُسنَدين إليه. راجع إدارة الأدوار.
وحدة تنظيمية	يحتاجه كل من يعمل ضمن جزء محدّد من هيكلك التنظيمي.
الزوّار المجهولون	قد يستخدم أشخاص لم يسجّلوا الدخول نموذجًا أو صفحة عامة. استخدم هذا الخيار بحذر.

وتظهر مجموعات الاستعلام، التي يُختار أعضاؤها وفق قاعدة محفوظة، بوصفها مجموعات أيضًا. راجع إدارة المجموعات.

على ماذا يمكنك منح الوصول

- **المنصة كلّها (مستوى النظام).** يحتاج كل شخص إلى مستوى على النظام، إذ يحدّد ما يستطيع فعله في كل مكان، وأيّ قوائم **الإدارة** تظهر له.
- **وحدة**، ومن خلالها كل كيانات البيانات التي تضمّها.
- **كيان بيانات**، وهو نوع واحد من المُدخلات، مثل الموظفين أو أرصدة الإجازات؛ ومن يملك وصولًا إلى كيان واحد يستطيع فتح وحدته، لكنه لا يرى فيها إلا ذلك الكيان.
- **معرض أو صفحة أو تقرير**، أي شاشة منشورة؛ فامنح مستوى «عرض» لمن ينبغي أن يتمكّن من فتحها.
- **خدمة**: من يستطيع تقديمها، ومن يستطيع متابعة طلباتها؛ وتعمل الخدمات بطريقة مختلفة قليلًا: راجع الخدمات وطلباتها.

بأي قدر: مستويات الوصول

المستوى	ما يتيحه	أين يمكنك منحه
مقيّد `Since 1.8`	لا يتيح شيئًا بمفرده، بل يُثبت أن الشخص عضو فيسري ما تمنحه له من وصول في مواضع أخرى. وعلى الوحدة أو الكيان، يؤدّي اختيار «مقيّد» إلى سحب الوصول الممنوح هناك.	مستوى النظام؛ وعلى الوحدة أو الكيان يعني «العودة إلى المستوى الأساسي».
عرض	يتيح رؤية تصميم الوحدة أو الكيان، وفتح المعارض والصفحات والتقارير التي جرت مشاركتها معه، **لكنه لا يُظهر المُدخلات نفسها** في الإدارة.	النظام، والوحدة، والكيان، والمعرض، والصفحة، والتقرير
مطور	يتيح بناء التصميم وتغييره – الحقول والمعارض والصفحات والسمات – دون رؤية المُدخلات.	النظام، والوحدة، والكيان
تعديل	يتيح كل ما يمنحه مستوى «مطور»، إضافةً إلى استعراض المُدخلات وفتحها وتغييرها في الإدارة.	النظام، والوحدة، والكيان
إدارة	يتيح تحكّمًا كاملًا في المنصة، بما في ذلك إدارة الأذونات.	مستوى النظام فقط

⚠ رؤية المُدخلات تتطلّب مستوى «تعديل»

لكي يستعرض شخصٌ قائمة مُدخلات كيانٍ أو يفتحها في **الإدارة**، يحتاج إلى مستوى **تعديل** على ذلك الكيان أو على وحدته، أو إلى «تعديل» أو «إدارة» على مستوى النظام؛ إذ لا يكفي مستوى «عرض»، ولو لمُدخل واحد. ومعظم المستخدمين لا يحتاجون إلى ذلك أصلًا، لأنهم يتعاملون مع المُدخلات عبر المعارض والصفحات والخدمات التي تشاركها معهم، ولكلٍّ منها إعدادات وصول خاصة بها.

كيف تتراكم المنح

- **المستوى الأعلى هو الغالب.** إذا كان لدى لينا مستوى «عرض» على كيان الموظفين مباشرةً، ومستوى «تعديل» عبر مجموعة الموارد البشرية، فمستواها الفعلي هو «تعديل».
- **لا يوجد «منع».** لا تسحب منحةٌ وصولًا تمنحه منحةٌ أخرى؛ ولسحب الوصول، احذف المنحة التي تمنحه، وتحقّق كذلك من مجموعات الشخص وأدواره.
- **حذف المنحة لا يحذف إلا تلك المنحة.** فإن ظلّ الشخص يحصل على الوصول عبر مجموعة أو دور أو مستوى النظام، احتفظ به.
- **مستوى إدارة لا يُحتسب إلا على النظام.** لا تمنح منحة «إدارة» على وحدة أو كيان شيئًا؛ فامنح هناك «عرض» أو «مطور» أو «تعديل» بدلًا منها.
- **المستويات الأعلى تشمل ما دونها.** يشمل مستوى «تعديل» أو «إدارة» على النظام كل وحدة وكل كيان، كما يشمل الوصول إلى وحدةٍ الكياناتِ التي تضمّها.

الخدمات وطلباتها

يُحدَّد من يرى طلبات الخدمة في الخدمة نفسها، لا عبر مستويات الوصول:

من	ما يرونه
جمهور الخدمة	يرون الخدمة في **دليل الخدمات** ويستطيعون تقديمها؛ وقد يكون الجمهور الجميع، أو المستخدمين المسجّلين فقط، أو قائمة من المستخدمين والمجموعات.
مقدّم الطلب	يرى طلباته هو في **الصادر**.
مالكو الخطوات	يرون الطلبات التي تصل إلى خطوة في سير العمل يملكونها هم أو تملكها مجموعتهم، وذلك في **الوارد**.
المتابِعون	يرون كل طلبات تلك الخدمة في **المتابعة**، دون أن يُطلب منهم أي إجراء عليها.

فإذا أردت أن تتابع مجموعة الموارد البشرية كل طلبات الإجازة، فاجعلها من **المتابِعين** في خدمة الإجازات. وتجد المثال الكامل في اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط.

مشاركة المعارض والصفحات والتقارير

يكون المعرض أو الصفحة أو التقرير المنشور إمّا متاحًا لكل من يستطيع الوصول إليه، وإمّا **مقيّدًا** بقائمة من المستخدمين والمجموعات. وحين تضيف مستخدمًا أو مجموعة إلى معرض أو صفحة أو تقرير، يتحوّل إلى الوضع «مقيّد»، فلا يفتحه إلا الأشخاص والمجموعات المدرجون في قائمته.

أين تدير الوصول

تجد كل شاشات الوصول ضمن **الإدارة › إدارة الوصول**، ولا تظهر لك هذه القائمة إلا إذا كان مستواك على النظام **إدارة**.

الشاشة	استخدمها من أجل
أذونات المدير	ضبط **مستوى النظام** لكل مستخدم ومجموعة (مقيّد، عرض، مطور، تعديل، إدارة).
أذونات وصول المستخدم	اختيار شخص واحد ورؤية كل ما يستطيع الوصول إليه ومصدر كل إذن لديه، ومنحه الوصول إلى المعارض والصفحات والتقارير والخدمات أو سحبه منه.
أذونات وصول المجموعة	اختيار مجموعة واحدة وإدارة وصولها إلى المعارض والصفحات والتقارير والخدمات، والاطلاع على أذوناتها الإدارية وحقولها الحسّاسة.
أذونات وصول الكائن	اختيار معرض أو صفحة أو تقرير أو خدمة بعينها، ورؤية من يستطيع فتحها.
الأذونات الحساسة	تحديد من يحقّ له رؤية الحقول المحجوبة مثل الرواتب. راجع الحقول الحسّاسة.
أذونات وصول المجهولين	تحديد ما يستطيع فتحه من لم يسجّلوا الدخول.

أما الوصول إلى وحدة أو كيان بيانات بعينه، فتديره من تبويب **الأذونات** الخاص بتلك الوحدة أو ذلك الكيان (**الإدارة › التطبيقات › الوحدات** أو **الكيانات**).

المهام

امنح الجميع مستوى أساسيًا

يُرفض وصول الشخص الذي لا يملك أي مستوى على النظام في كل مكان تقريبًا؛ لذا امنح كل شخص مستوى **مقيّد** على الأقل، ويكون ذلك عادةً عبر مجموعة ينتمي إليها الجميع.

1. افتح **الإدارة › إدارة الوصول › أذونات المدير**.
2. اختر تبويب **المجموعات**، ثم اختر **إضافة**.
3. في **حدد مجموعة للإضافة**، اختر المجموعة. وفي **حدد مستوى الصلاحية**، اختر **مقيّد**، ثم اختر **تأكيد**.

بعد ذلك، ارفع مستوى كل فريق بحسب حاجته؛ فامنح مثلًا مسؤولي تقنية المعلومات مستوى **إدارة**، وبُناة التطبيقات مستوى **مطور**.

امنح مجموعة وصولًا إلى وحدة أو كيان بيانات

مثال: مجموعة الموارد البشرية مسؤولة عن تحديث مُدخلات الموظفين.

1. تأكّد من أن لمجموعة الموارد البشرية مستوى على النظام (راجع امنح الجميع مستوى أساسيًا)، إذ لا تعرض شاشات الوحدات والكيانات إلا المستخدمين والمجموعات التي لديها مستوى بالفعل.
2. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح **الموظفون**. (ولمنح الوصول إلى وحدة كاملة، افتح **الإدارة › التطبيقات › الوحدات** وافتح الوحدة بدلًا من ذلك.)
3. افتح تبويب **الأذونات**، ثم انتقل إلى **المجموعات**.
4. في صف **الموارد البشرية**، اضبط **مستوى الصلاحية** على **تعديل**، وأكّد التغيير.

تظهر لك المستويات «مقيّد» و«عرض» و«مطور» و«تعديل»، ولا يقلّ أيٌّ منها عن المستوى الذي تملكه المجموعة أصلًا على النظام، أو – عند ضبط صلاحية كيان – على الوحدة التي تضمّه. أما المجموعات التي لديها **تعديل** أو **إدارة** على النظام فلا تظهر في القائمة، لأنها تصل إلى كل شيء أصلًا.

امنح مجموعة وصولًا إلى معرض أو صفحة أو تقرير أو خدمة

مثال: اسمح لمجموعة الموارد البشرية بفتح تقرير «عدد الموظفين حسب القسم».

1. افتح **الإدارة › إدارة الوصول › أذونات وصول المجموعة**.
2. في **اختر المجموعة**، اختر **الموارد البشرية**، وابقَ في تبويب **أذونات المجموعة**.
3. اختر **إضافة إذن**.
4. في **الكائن**، اختر التقرير؛ وإذا كان الكائن خدمة، فاختر كذلك **جمهور الخدمة** (يستطيعون تقديمها) أو **المتابِعين** (يرون كل طلباتها).
5. احفظ.

ينبّهك مربع الحوار حين يوشك الكائن أن يتحوّل إلى الوضع «مقيّد»، فمن تلك اللحظة لا يفتحه إلا الأشخاص والمجموعات المدرجون في قائمته.

> ⚠ **مشكلة معروفة: قد لا يظهر المعرض في الشريط الجانبي عند منح إذن الوصول إليه من هنا**
>
> عند منح مجموعة أو مستخدم إذن الوصول إلى معرض من **أذونات وصول المجموعة** أو **أذونات وصول المستخدم**، قد لا يظهر المعرض (ووحدته) في الشريط الجانبي لديهما إلا بعد إعادة فتح المعرض في مصمّم المعرض. ولإظهاره، امنح إذن الوصول من نافذة **الأذونات** الخاصة بالمعرض نفسه بدلًا من ذلك، أو افتح المعرض مرة واحدة في مصمّم المعرض (دون الحاجة إلى الحفظ). وقد يلزم أن يُحدّث المستخدم الصفحة ليظهر له المعرض.

غيّر الوصول أو احذفه

- **مستوى النظام:** في **أذونات المدير**، غيّر **مستوى الصلاحية** في الصف، أو اختر أيقونة سلة المهملات لحذفه، ثم أكّد.
- **وحدة أو كيان:** في تبويب **الأذونات** الخاص بالوحدة أو الكيان، غيّر **مستوى الصلاحية** ثم أكّد؛ ولسحب الوصول، أعده إلى **مقيّد**، فتُحذف المنحة على تلك الوحدة أو ذلك الكيان، ويعود الشخص أو المجموعة إلى مستوى النظام الخاص به.
- **معرض أو صفحة أو تقرير أو خدمة:** في **أذونات وصول المجموعة** أو **أذونات وصول المستخدم**، استخدم إجراء **تعديل** في الصف، أو إجراء الحذف لإزالته.
- **كل ما تملكه مجموعة واحدة:** في **أذونات وصول المجموعة**، اختر المجموعة وافتح تبويب **أذونات الإدارة** الخاص بها لتغيير كل منحة أو حذفها.

يُزيل حذف المنحة ذلك الإذن، لكنه لا يمنع الشخص من الوصول؛ فإن ظلّ يحصل عليه عبر مجموعة أو دور أو مستوى النظام، احتفظ به.

وإذا حذفت مستوى النظام الوحيد لشخص ما، فقدَ الوصول إلى كل شيء تقريبًا. ولسحب كل وصول الشخص عند مغادرته، عطّل حسابه أو أرشِفه بدلًا من ذلك. راجع إدارة المستخدمين.

تحقّق مما يستطيع شخص ما الوصول إليه

1. افتح **الإدارة › إدارة الوصول › أذونات وصول المستخدم**.
2. في **اختر المستخدم**، اختر الشخص.
3. راجع التبويبات **أذونات المستخدم** و**أذونات الإدارة** و**الحقول الحساسة**.

لكل إذن، يبيّن **نوع الإذن** كيف حصل عليه الشخص – **إذن مُعطاة مباشرة**، أو **إذن موروثة من مجموعة**، أو **إذن موروثة لجميع المستخدمين المصادق عليهم**، أو **إذن موروثة من التفويض**، أو **إذن موروثة للمستخدم المجهول** – ويعرض **مكتسبة عن طريق** اسم المجموعة أو الدور، فيما تبيّن **الإجراءات المتاحة** ما يتيحه الإذن له.

مثال تطبيقي: قسم الموارد البشرية

الحاجة	ما تضبطه
يستطيع الجميع تسجيل الدخول واستخدام المعارض والصفحات التي تُشارَك معهم	**مقيّد** على مستوى النظام لمجموعة تضمّ جميع الموظفين.
يستطيع الجميع أيضًا تقديم الطلبات واتخاذ الإجراءات عليها في **الوارد**	**عرض** على مستوى النظام لتلك المجموعة بدلًا من ذلك؛ فمن كان مستواه على النظام **مقيّد** لا تظهر له قائمة **الخدمات** (لا **دليل الخدمات** ولا **الصادر** ولا **الوارد**). و**عرض** أدنى مستوى تظهر معه هذه القائمة، ويُظهر معها أيضًا قائمة **الإدارة** بصورة مختصرة.
يحدّث موظفو الموارد البشرية مُدخلات الموظفين	**تعديل** على كيان الموظفين لمجموعة **الموارد البشرية**.
يستطيع مديرو الموارد البشرية فتح تقرير عدد الموظفين	أضِف التقرير إلى مجموعة دور **مدير الموارد البشرية** في **أذونات وصول المجموعة**.
تتابع الموارد البشرية كل طلبات الإجازة	مجموعة **الموارد البشرية** ضمن **المتابِعين** في خدمة الإجازات – راجع دليل الخطوات.
لا يرى الرواتب إلا مديرو الموارد البشرية	منحة حقل حسّاس على حقل الراتب لدور مدير الموارد البشرية – راجع الأذونات الحساسة.
لا يستطيع أحد في الموارد البشرية تغيير تصميم المنصة	لا تمنح الموارد البشرية **مطور** أو **تعديل** أو **إدارة** على مستوى النظام.

من المفيد أن تعرف

لا يمكنك منح أكثر مما تملك `Since 1.8`

ما لم يكن مستواك على النظام **إدارة**، فلا يمكنك منح مستوى يعلو مستواك أنت على تلك الوحدة أو ذلك الكيان، ولا تغيير منحة تعلو مستواك أو حذفها؛ وتعرض المنصة حينئذ الرسالة: "You cannot grant, change or revoke access above your own level."

لا تستطيع الأتمتة منح أكثر مما يملكه مؤلّفها `Since 1.10`

يمكن للأتمتة (التفاعل) أن تمنح أذونات أو تسحبها. وحين يحفظ أحدهم أتمتةً من هذا النوع، تتحقّق المنصة من أنه يملك أصلًا الوصول الذي ستمنحه، أما سحب الوصول فيتطلّب مستوى **إدارة** على ذلك الكائن؛ فإن لم يتحقّق ذلك، لا تُحفَظ الأتمتة.

التفويض وحقوق الإدارة `Since 1.10`

ينقل التفويض الذي يسمح بكل شيء كل وصول المفوِّض باستثناء مستوى **إدارة** على النظام، ما لم يُسمح بالإدارة صراحةً في ذلك التفويض. راجع التفويض.

تسري التغييرات فورًا

يسري أي تغيير في الأذونات عند الإجراء التالي الذي يتّخذه الشخص، في أي مكان على المنصة. وإذا ظلّت قوائمه على حالها، فاطلب منه تحديث الصفحة.

الوصول المجهول

تعرض أذونات الوصول المجهول وروابط المشاركة المجهولة البيانات لأي شخص دون تسجيل دخول؛ فراجعها بعناية قبل استخدامها مع أي محتوى حسّاس.

شخصان يحرّران المُدخل نفسه

حين يحرّر أحدهم مُدخلًا، يمكن للمنصة أن تقفله كي لا يكتب الآخرون فوق تغييراته؛ فيرى الآخرون أنه مقفل، ويحتفظ المُدخل بتاريخ أقفاله.

فحص تخويل ثانٍ قد يشغّله المشغّل `Since 1.10`

يستطيع المشغّل لديك تفعيل فحص في الخلفية يقارن قرارات الوصول في المنصة بقرارات نظام ثانٍ. ويقتصر هذا الفحص على القياس، إذ لا يغيّر أبدًا أذونات أحد، ولا يتطلّب ضبط أي إعداد في **الإدارة**.

الحقول الحسّاسة

يستطيع باني التطبيق أن يضبط بعض الحقول، مثل الراتب، على **حساس** أو **تشفير**، وتبقى قيمها محجوبة حتى عمّن يستطيع فتح المُدخل، بمن فيهم أصحاب مستوى «إدارة»، إلى أن تمنح شخصًا أو مجموعة منحة حقل حسّاس؛ وحتى عندئذ، يجب على الشخص تأكيد هويته قبل أن تظهر القيمة. وتُدير هذه المنح من **الإدارة › إدارة الوصول › الأذونات الحساسة**، أو من تبويب **الحقول الحساسة** الخاص بالمستخدم أو المجموعة، ويمكن أن يكون للمنحة تاريخ انتهاء تُحذف بعده تلقائيًا. وتجد الإجراء الكامل في الأذونات الحساسة.

استكشاف الأخطاء وإصلاحها

«لا يرى المستخدم وحدة أو كيانًا.» افتح **أذونات وصول المستخدم** لهذا الشخص وابحث عن الوحدة أو الكيان؛ فإن لم تجده، فامنح الوصول لإحدى مجموعاته (أو له هو) من تبويب **الأذونات** في الوحدة أو الكيان، وتحقّق كذلك من أن لديه مستوى على النظام، **مقيّد** على الأقل.

«يرى المستخدم الكيان لكنه لا يرى مُدخلاته.» تتطلّب رؤية المُدخلات في **الإدارة** مستوى **تعديل**؛ فإمّا أن تمنحه مستوى «تعديل»، وإمّا – وهو الأنسب لمعظم المستخدمين – أن تشارك معه معرضًا أو صفحة تعرض المُدخلات التي يحتاجها.

«لا يرى المستخدم خدمة في دليل الخدمات.» إمّا أنه ليس ضمن **جمهور الخدمة**، وإمّا أن الخدمة غير نشطة. أضِف مجموعته إلى **جمهور الخدمة** من **أذونات وصول المجموعة**، أو اطلب من باني الخدمة التحقّق من إعدادات ظهورها.

«سحبتُ الوصول، لكن الشخص ما زال يراه.» يحصل الشخص في هذه الحالة على الوصول بطريقة أخرى؛ ففي **أذونات وصول المستخدم**، راجع **نوع الإذن** و**مكتسبة عن طريق**، ثم احذف المنحة من تلك المجموعة أو ذلك الدور، أو أخرِج الشخص

من المجموعة.

«المستوى الذي أريده غير موجود في القائمة.» يتاح مستوى «إدارة» على مستوى النظام فقط. وعلى الكيان، لا يمكنك اختيار مستوى أدنى مما تملكه المجموعة على الوحدة. وما لم يكن مستواك على النظام «إدارة»، فلا يمكنك منح أكثر مما تملكه أنت.

«لا يرى المستخدم قيمة محجوبة.» يحتاج المستخدم إلى منحة حقل حسّاس، وعليه أن يؤكّد هويته في كل مرة. راجع الأذونات الحساسة.

للتعمّق أكثر

لمطوّري التكامل: واجهة برمجة الأذونات (Permissions API) [التكامل والتوسعة › واجهة الأذونات البرمجية] — سجلات المنح، والمستويات، ونقاط النهاية، والقواعد التي يفرضها كل استدعاء · لبُناة التطبيقات: الحقول الحسّاسة [بناء التطبيقات › حماية حقل] · لمهندسي المنصة: المحرّك: الأذونات والمصوّتون

الأذونات الحساسة

> **التوفّر**
>
> Since 1.8.

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتبيّن لك كيف تحدّد من يحق له قراءة القيم المحمية، مثل الرواتب وأرقام الهوية الوطنية: كيف تمنح هذا الحق، وكيف تحدّده بمدة، وكيف تراجع من يتمتع به، وكيف تسحبه.

يستطيع مصمّم الكيان أن يضع علامة **حساس** على حقل بعينه – راتب، أو رقم وطني، أو حساب بنكي. عندئذٍ يُخفي أسس قيمة ذلك الحقل خلف القناع `****` عن الجميع، ولا يُظهر القيمة الحقيقية إلا لمن منحتهم حق قراءتها صراحةً.

`Since 1.10` ويمكن بدلًا من ذلك وضع علامة **مشفَّر** على الحقل، فتُخزَّن قيمته بصورة مشوَّشة في قاعدة البيانات بدلًا من إخفائها عند الإخراج. ويُمنح الوصول إليه من الشاشات نفسها، وبالمنحة نفسها – راجع الحقول المشفَّرة تستخدم المنحة نفسها.

ويُستثنى حقل واحد من ذلك بحكم التصميم: **لا يمكن وضع علامة حساس على حقل العنوان الرئيسي للكيان**، كما أن الحقل الحساس أصلًا لا يظهر ضمن الحقول المرشّحة لتكون العنوان الرئيسي. فالعنوان الرئيسي يُعرض غير مُقنَّع في كل موضع يُشار فيه إلى المُدخل باسمه، ولذلك فإن السماح باستخدام حقل حساس فيه سيؤدي إلى تسريب القيمة. `Since 1.8`

ومن شاشة **الإدارة › إدارة الوصول › الأذونات الحساسة** تمنح هذا الحق وتسحبه. فهي تعرض في شاشة واحدة كل منحة سارية لحقل حساس في المساحة، كما يمكنك الوصول إلى المنح نفسها من شاشة أذونات الوصول الخاصة بمستخدم واحد أو بمجموعة واحدة. ويغطّي هذا الدليل الشاشات الثلاث جميعها وما يقابلها في تطبيق الهاتف المحمول.

بُعد منفصل عن الأذونات الاعتيادية

تجيب الأذونات الاعتيادية عن سؤال «ما الذي يجوز لهذا الشخص فعله بهذا *الكائن*؟» – وحدة، أو كيان، أو معرض، أو تقرير. أما الإذن الحساس فيجيب عن سؤال أكثر تحديدًا: «هل يجوز لهذا الشخص قراءة *قيمة* هذا الحقل الواحد؟» ويُقيَّم كلٌّ منهما على حدة:

- المستخدم الذي لديه مستوى **إدارة** على كيان يظل يرى `****` في حقوله الحساسة ما لم يكن لديه إذن حساس لتلك الحقول.
- **لا يتجاوزه أي دور.** فالحقل يُخفى عن مسؤول النظام ذي الصلاحيات الكاملة تمامًا كغيره. ولا يوجد مستوى «يرى كل شيء»، فالسبيل الوحيد لقراءة قيمة حساسة هو الحصول على منحة لقراءتها.
- منح إذن حساس يتيح **قراءة** قيمة ذلك الحقل ولا شيء غير ذلك، ولا يوسّع أبدًا نطاق ما يستطيع الشخص الوصول إليه في مواضع أخرى.
- وتسري إزالة الإذن فورًا، عند القراءة التالية.

وإدارة الأذونات الحساسة هي بحد ذاتها صلاحية ذات امتياز: فعنصر القائمة **الأذونات الحساسة** لا يظهر إلا لـ**مسؤولي النظام**. ومنحة الحقل الحساس والإذن الاعتيادي للشخص نفسه قائمان جنبًا إلى جنب؛ فمنح شخص إذنًا اعتياديًا لا يغيّر أبدًا منح الحقول الحساسة الخاصة به.

تفاصيل تقنية

تتطلب العمليات التي تنفّذها هذه الشاشات صلاحيات على مستوى النظام: فقراءة قائمة المنح تتطلب مستوى **عرض**، وإنشاء منحة أو تغييرها أو إزالتها يتطلب مستوى **مطور** أو أعلى.

نطاقات الحقول الحساسة

لا تشير المنحة إلى الحقل باسمه المعروض، بل تحمل **نطاقًا** يحدّد مدى اتساعها. افهم هذا النطاق قبل إضافة أول منحة، لأن اختيار كيان أو وحدة في أداة الاختيار يمنح وصولًا أوسع بكثير من اختيار حقل واحد.

يُعرَّف كل حقل حسّاس عبر المساحة (space) بأكملها بسلسلة **نطاق (scope)** مرجعية واحدة. ويُبنى النطاق من الأسماء المُنمّطة (أسماء الآلة)، مفصولةً بالرمز `/` :

```
<module>/<entity>/<field>
```

وبالنسبة إلى حقل يقع داخل **كتلة (block)**، يكون المقطع الأخير هو الاسم المُنمّط ذا الصيغة المنقوطة `block.subfield` – مثل `hr/employee/payroll.iban` .

تحمل المنحة نطاقًا كما يحمل الحقل نطاقًا، وتُقارَن السلسلتان **مقطعًا بمقطع**. ويجب أن يكون لكليهما العدد نفسه من المقاطع المفصولة بالرمز `/` كي تحصل المطابقة أصلًا. ويجوز أن يكون أي مقطع هو الرمز البديل (wildcard) `*` ، فيطابق أيًّا كان ما يقع في ذلك الموضع:

نطاق المنحة	ما الذي يشمله
`hr/employee/salary`	ذلك الحقل وحده تحديدًا – منحة **مباشرة**.
`hr/employee/payroll.iban`	الحقل الفرعي `iban` داخل الكتلة `payroll` في الكيان `employee` .
`hr/employee/*`	كل حقل حسّاس في الكيان `employee` – منحة **بالرمز البديل على مستوى الكيان**.
`hr/*/*`	كل حقل حسّاس في أي موضع ضمن الوحدة `hr` – منحة **بالرمز البديل على مستوى الوحدة**.
`hr/*/salary`	الحقل `salary` في كل كيان ضمن الوحدة `hr` .

المنحة التي يسمّي نطاقُها حقلًا بعينه هي منحة **مباشرة** على ذلك الحقل؛ أما المنحة التي تصل إلى الحقل عبر مقطع بالرمز البديل فهي منحة **موروثة**. وكلتاهما تمنحان حق القراءة نفسه تمامًا – والفارق هو *أين* تقيم المنحة، ومن ثمّ أين تذهب لتعديلها أو إلغائها.

ولا تُكتب النطاقات يدويًا. إذ يعرض مُحدِّد النطاق المساحةَ على هيئة شجرة **وحدة › كيان › حقل**: فاختيار حقل طرفي يؤلّف النطاق الملموس ذا المقاطع الثلاثة، بينما يؤلّف اختيار عقدة كيان أو عقدة وحدة النطاقَ المقابل بالرمز البديل الذي يشمل كل ما تحتها.

الحقول المشفَّرة تستخدم المنحة نفسها `Since 1.10`

يستطيع المصمّم أن يضع على الحقل علامة **مشفَّر** بدلًا من «حساس». ويكمن الفارق في موضع الحماية: فالحقل الحساس يُخزَّن بصورة عادية وتُقنَّع قيمته قبل عرضها للقارئ، أما الحقل **المشفَّر** فيُخزَّن نصًا مشفَّرًا في قاعدة البيانات نفسها. ولا يمكن أن يكون الحقل كليهما، فالخياران متنافيان، وتفعيل أحدهما في محرّر الحقل يعطّل الآخر.

وبالنسبة إليك بصفتك المسؤول عن منح الوصول، لا يتغيّر شيء تقريبًا:

- **إنها المنحة نفسها.** فالوصول إلى الحقل المشفَّر يُمنح بالإذن الحساس نفسه، وضمن تسلسل النطاق نفسه: وحدة ← كيان ← حقل، ومن الشاشات الثلاث نفسها. فلا يوجد نوع ثانٍ من المنح ولا «إذن فك تشفير» منفصل تديره.
- **الحقول المشفّرة في أداة الاختيار نفسها.** فالحقل المشفَّر غير الحساس يظهر تحت **اختر حقلاً حساساً** إلى جانب الحقول الحساسة، في كل مربع حوار للإضافة – في الصفحة على مستوى المساحة، وتبويب المستخدم، وتبويب المجموعة.
- **إزالة المنحة تُلغي الوصول إلى فك التشفير فورًا**، تمامًا كما في الحقل الحساس، وتعمل فترة الصلاحية بالطريقة نفسها.

أما ما *يختلف* فعلًا فهو الإجراء الذي يتبعه صاحب المنحة بعد ذلك، وهو مشروح في ما الذي يراه صاحب المنحة فعلًا: إذ يتطلّب كشف قيمة مشفَّرة تحققًا من الهوية صالحًا للاستخدام مرة واحدة ولمدة قصيرة في كل مرة، بينما يفتح كشف قيمة حساسة جلسة كشف تستمر مدة أطول.

قائمة المنح على مستوى المساحة

تعرض صفحة الأذونات الحساسة **كل** منحة سارية في المساحة، بصف واحد لكل زوج (نطاق، مستخدم أو مجموعة):

العمود	ما يعرضه
النطاق	سطران: سياق الوحدة/الكيان في الأعلى، وتحته الحقل (أو الكيان أو الوحدة التي تشملها المنحة إذا كانت تستخدم الرمز البديل).
نوع النطاق	**حقل** أو **كيان** أو **وحدة** – يبيّن مدى شمول المنحة، لتعرف بنظرة سريعة مدى اتساع النطاق في الصف.
اسم المستخدم أو المجموعة	الشخص أو المجموعة الحاصلة على المنحة.
مدة الصلاحية	نهاية فترة الصلاحية، معروضةً بتنسيق التاريخ والمنطقة الزمنية الخاصين بك. والخانة الفارغة تعني أن المنحة لا تنتهي أبدًا.
الإجراءات	تعديل مدة الصلاحية، أو إزالة المنحة.

وفوق الجدول مربع بحث يرشّح النتائج فورًا بالبحث في جميع الأعمدة المعروضة، متجاهلًا حالة الأحرف والمسافات في بداية عبارة البحث ونهايتها.

والقائمة **غير** مرشَّحة عمدًا بحسب فترة الصلاحية: فالمنحة التي لم يحِن تاريخ بدايتها بعد تظهر هنا أيضًا، كي تتمكن من رؤيتها وتعديلها قبل أن تصبح سارية.

إضافة منحة

1. افتح **الإدارة › إدارة الوصول › الأذونات الحساسة** واختر **إضافة إذن**.
2. تحت **النطاق**، افتح **اختر حقلاً حساساً** واختر من الشجرة وفق التسلسل وحدة ← كيان ← حقل. اختر حقلًا لمنح الوصول إلى حقل واحد، أو اختر كيانًا أو وحدة لمنح الوصول إلى كل ما يندرج تحتهما.
3. تحت **اختر مستخدمين** و**اختر مجموعات**، حدّد من سيحصلون على المنحة. ويمكنك اختيار عدة عناصر من كل نوع دفعة واحدة، فيحصل كل شخص أو مجموعة على منحة مستقلة للنطاق نفسه.
4. اضبط **مدة الصلاحية** إن أردت (راجع المنح المحدّدة المدة). واتركها فارغة لتستمر المنحة إلى أن تزيلها.
5. احفظ.

وإذا كان أحد من اخترتهم لديه أصلًا منحة سارية على ذلك النطاق، ينبّهك مربع الحوار قبل الحفظ ويتخطّى ذلك الطرف، فلا تُنشأ أبدًا منحتان متنافستان للزوج نفسه.

تعديل مدة صلاحية المنحة

يفتح إجراء التعديل في الصف المنحةَ مع **إتاحة تعديل مدة الصلاحية وحدها**. أما النطاق والمستخدم أو المجموعة الحاصلة على المنحة فيظهران مقفلين: فالمنحة إقرار يخص طرفًا واحدًا ونطاقًا واحدًا، وتغيير أيٍّ منهما قد يُنشئ نسخة مكررة من منحة قائمة دون تنبيه. ولتغيير أيٍّ منهما، أزِل المنحة وأضِف المنحة التي تريدها.

ومسح المدى الزمني ثم الحفظ يزيل فترة الصلاحية كليًا، فتعود المنحة بلا تاريخ انتهاء.

إزالة منحة

يطلب إجراء سلة المهملات في الصف تأكيدًا – *«لن يتمكن المستخدم أو المجموعة بعد ذلك من الوصول إلى هذا الحقل الحساس»* – ثم **يحذف نهائيًا** سجل المنحة. ويزول الوصول عند القراءة التالية، ولا يتوفر خيار للتراجع ولا نسخة مؤرشفة في هذه الشاشة. فإذا كنت قد تحتاج إلى إعادة الوصول لاحقًا، فإعادة إضافة المنحة أيسر من محاولة استرجاعها.

وإزالة منحة في تطبيق الهاتف المحمول لها الأثر نفسه تمامًا – راجع إدارة المنح من تطبيق الهاتف المحمول.

الأذونات الحساسة لمستخدم واحد

تضم شاشة أذونات الوصول الخاصة بالمستخدم تبويب **الحقول الحساسة** إلى جانب أذونات المستخدم وأذونات الإدارة الاعتيادية الخاصة به. ويجيب هذا التبويب عن سؤال «ما البيانات الحساسة التي يستطيع هذا الشخص قراءتها فعلًا؟»، وهو سؤال يختلف عن «ما الذي منحته لهذا الشخص مباشرةً؟».

ويسرد التبويب **كلا** نوعَي المنح:

نوع الإذن	المعنى
إذن مُعطاة مباشرة	المنحة تحدّد هذا المستخدم بوصفه صاحبها.
المجموعة	المنحة تخصّ مجموعة ينتمي إليها المستخدم، ويكتسبها بحكم عضويته فيها. ويبيّن عمود **مكتسبة عن طريق** اسم تلك المجموعة.

ويظهر النطاق الذي يكتسبه المستخدم بالطريقتين معًا مرتين، مرة لكل طريقة، لأن مدة بقاء كل صف تختلف عن الآخر: فإزالة عضوية المجموعة تُنهي أحدهما وتُبقي الآخر قائمًا.

ولا تتاح إجراءات التعديل والإزالة هنا إلا للصفوف **المباشرة**. أما الصف الموروث فلا تتاح له إجراءات، لأن المنحة تخصّ المجموعة لا المستخدم. ولتعديلها، افتح المجموعة المذكورة في «مكتسبة عن طريق» وأدِر المنحة هناك، أو اقبل انطباقها على كل عضو في تلك المجموعة.

وعندما تضيف منحة من هذا التبويب، تستبعد أداة اختيار الحقول **النطاقات التي يحملها هذا المستخدم فعليًا**، مباشرةً أو عبر أي من مجموعاته، فلا يمكنك إضافة منحة ثانية عن غير قصد لوصول يملكه أصلًا.

ويتيح لك عنصر **تحديث** في التبويب إعادة تحميل القائمة دون مغادرة الشاشة. وفترة الصلاحية اختيارية: يمكنك حفظ منحة بلا تاريخ انتهاء، أما ملء الفترة جزئيًا أو تحديد فترة منقضية أصلًا فيمنع **حفظ**.

الأذونات الحساسة لمجموعة واحدة

تضم شاشة أذونات الوصول الخاصة بالمجموعة اللوحة نفسها لعرض منح المجموعة. وكل ما يُسرد هنا **مباشر** – فالمجموعة لا ترث أذونات حساسة من مجموعة أخرى – وكل منحة تنطبق على كل عضو حالي في المجموعة.

- **إضافة** تفتح مربع الحوار نفسه، وتستبعد أداة الاختيار النطاقات التي تحملها المجموعة أصلًا. وفترة الصلاحية اختيارية هنا.
- **إزالة تحذف** المنحة نهائيًا في تطبيق الويب، مع طلب التأكيد نفسه المستخدم في القائمة على مستوى المساحة. ويفقد كل عضو في المجموعة الوصول إلى ذلك الحقل فورًا. وهذا حذف لا أرشفة، ولا يمكن استعادة المنحة. (ويتبع التبويب المقابل في تطبيق الهاتف المحمول السلوك نفسه – راجع إدارة المنح من تطبيق الهاتف المحمول.)
- ويعيد عنصر التحديث تحميل القائمة، وتُعرض حالات التحميل وخلوّ القائمة والخطأ ضمن اللوحة مع خيار إعادة المحاولة.

ومنح المجموعة هو الخيار الأسهل صيانةً حين يحتاج عدة أشخاص إلى الحقل نفسه: إذ يتغيّر الوصول تبعًا لتغيّرات العضوية، ويكون أمامك صف واحد لإبطال المنحة بدلًا من صفوف كثيرة.

إدارة المنح من تطبيق الهاتف المحمول `Since 1.8`

الشاشات الثلاث أعلاه متاحة أيضًا في تطبيق الهاتف المحمول، فيمكنك إضافة منحة أو تمديدها أو سحبها من الهاتف:

الواجهة	بوابة الويب	تطبيق الهاتف المحمول
قائمة المنح على مستوى المساحة	صفحة إدارة **الأذونات الحساسة**	شاشة **أذونات الوصول إلى البيانات الحساسة**، وهي آخر عنصر في قائمة أذونات الوصول
مستخدم واحد	تبويب **الحقول الحساسة** في شاشة أذونات وصول المستخدم	تبويب **الحقول الحساسة** في شاشة وصول المستخدم
مجموعة واحدة	تبويب **الحقول الحساسة** في شاشة أذونات وصول المجموعة	تبويب **الحقول الحساسة** في شاشة وصول المجموعة

ولكل واجهة على الهاتف المحمول ورقة للإضافة وأخرى للتعديل تقتصر على مدة الصلاحية. وتختار النطاق عبر شجرة الاختيار نفسها **وحدة › كيان › حقل** المستخدمة في أداة الاختيار على الويب؛ فالمنح التي تُنشئها على الهاتف هي المُدخلات نفسها التي تسردها صفحات الويب. كما تنبّهك الشاشة على مستوى المساحة في الهاتف المحمول، قبل الحفظ، إذا كان أحد من اخترتهم مشمولًا أصلًا بمنحة قائمة على ذلك النطاق.

- **إزالة المنحة تعني الشيء نفسه في التطبيقين:** إذ تُحذف المنحة نهائيًا، دون تراجع.
- **فترة الصلاحية تتطلب التاريخين معًا أو لا شيء منهما.** فكل مربع حوار للإضافة، على الويب وعلى الهاتف المحمول، يمنع **حفظ** إلى أن تحدّد التاريخين كليهما أو تتركهما فارغين.
- في شاشة المجموعة على الهاتف المحمول، استخدم زر الإضافة العائم ما دام تبويب **الحقول الحساسة** مفتوحًا، فهو يفتح ورقة إضافة الحقل الحساس.

الأذونات الموروثة

لا تعرض إعدادات الحقل نفسه إلا الأشخاص الممنوحين ذلك الحقل **تحديدًا**. أما من يستطيع الوصول إليه عبر منحة بالرمز البديل على مستوى الكيان أو الوحدة فلا يظهر هناك، وهذه هي الحالة الأرجح أن تفاجئك أثناء المراجعة.

ويسدّ هذه الفجوة مربع حوار **الأذونات الموروثة**، الذي يمكنك فتحه من الإعدادات المتقدمة للحقل بجوار مفتاح «حساس». فهو يسرد المستخدمين والمجموعات القادرين على قراءة الحقل عبر منحة بالرمز البديل، لا عبر منحة على الحقل نفسه.

- لا يظهر هذا العنصر إلا بعد وضع علامة على الحقل بأنه حساس **و**وجود مستخدم أو مجموعة واحدة على الأقل يملك إذنًا موروثًا للوصول إليه.
- وعند فتحه، يعيد تحميل القائمة أولًا، فلا تتصرف أبدًا بناءً على معلومات قديمة.

- ومربع الحوار نفسه **للقراءة فقط**: يعرض المستخدمين بأسمائهم وعناوين بريدهم الإلكتروني، والمجموعات بأسمائها، دون أي إجراءات للتعديل أو الإزالة فيه. إذ يجب تغيير المنحة الموروثة في موضعها، ضمن نطاقها بالرمز البديل على مستوى الكيان أو الوحدة في القائمة على مستوى المساحة.

راجع قائمة الحقل المباشرة ومربع حوار الأذونات الموروثة معًا؛ فلا تتضح لك هوية من يستطيع رؤية تلك القيمة إلا بالاطلاع عليهما معًا.

الاطلاع على سجل المنحة الكامل لحاملها `Since 1.8`

حدّد مستخدمًا أو مجموعة في قائمة الأذونات الموروثة لفتح لوحة للقراءة فقط تعرض المنحة التي تتيح لذلك المستخدم أو لتلك المجموعة الوصول إلى هذا الحقل: **النطاق**، و**نوع النطاق**، و(للمستخدمين) **نوع الإذن** و**مكتسبة عن طريق**، و**مدة الصلاحية**. وعندما يصل المستخدم أو المجموعة إلى الحقل عبر أكثر من منحة، تعرض اللوحة المنحة على مستوى الكيان بدلًا من المنحة على مستوى الوحدة، مع تجاهل المنح المنتهية الصلاحية.

وإذا فقد المستخدم أو المجموعة المنحة قبل فتح اللوحة، فإنها تعرض: *لم يعد بإمكان هذا المستخدم أو المجموعة الوصول إلى هذا الحقل الحساس*. وإذا فشل الاستعلام، فاختر **إعادة المحاولة**.

وينقلك زر **توسيع** في اللوحة مباشرةً إلى المُدخل الكامل القابل للتعديل لذلك المستخدم أو لتلك المجموعة – أي إلى تبويب الحقول الحساسة في شاشة مستخدم واحد أو مجموعة واحدة أعلاه، عبر رابط مباشر – وبمجرد اكتمال الانتقال فعلًا، تُغلق اللوحة ومربع حوار الأذونات الموروثة خلفها معًا، فلا تبقى أمامك لوحتان متراكبتان فوق التبويب الذي فتحته للتو.

المنح المحدّدة المدة

يمكن أن تكون للمنحة **فترة صلاحية** بدلًا من أن تستمر إلى أن يتذكّر أحدهم إبطالها:

ما تضبطه	الأثر
لا تاريخ	لا تنتهي المنحة أبدًا، وهذا هو الوضع الافتراضي.
تاريخ نهاية فقط	تسري المنحة من الآن حتى ذلك التاريخ.
التاريخان معًا	تسري المنحة خلال الفترة المحدّدة كاملةً. وقبل تاريخ البداية، تكون مدرجة لكنها لا تمنح أي إذن.

ويجب أن يكون تاريخ النهاية في المستقبل عند إنشاء المنحة، إذ ترفض المنصة أي منحة انتهت صلاحيتها بالفعل.

وعند حلول تاريخ النهاية، **يؤرشف أسس المنحة تلقائيًا** عبر مؤقّت مُعدّ مسبقًا، ويسري السحب فورًا: تُمسح الأذونات المخبوءة للمستخدم، ويُعاد حساب حالة تقييد الحقل، وتُستبعد المنحة المؤرشفة من كل استعلام لاحق عن الأذونات. ولا يلزم أي إجراء يدوي، ولا يحتاج أحد إلى تذكّر التاريخ.

ويترتّب على إزالة المنحة يدويًا قبل تاريخ نهايتها الأثر الفوري نفسه تمامًا. وفي الحالتين، تؤدي إعادة منحها للطرف نفسه لاحقًا إلى إنشاء منحة جديدة، ولا تعيد تفعيل القديمة ضمنيًا.

استخدم فترة صلاحية للوصول المؤقت فعلًا – كأن تتيح لمراجِع الاطّلاع على حقل الراتب طوال مدة مهمة – ولا تتركها مفتوحة إلا للوصول الذي يشكّل جزءًا من عمل الشخص الدائم.

ما الذي يراه صاحب المنحة فعلًا

المنحة ضرورية، لكنها وحدها **لا** تكفي لكشف القيمة. لذا وضّح للمستخدم ما يمكنه توقّعه عند منحه إياها:

- من دون منحة، تظهر القيمة `****` في كل موضع يمكن أن تظهر فيه – أعمدة القوائم، وتفاصيل المُدخل، والسجل التاريخي للمُدخل، والتقارير، والتصدير. ويظل بإمكان المستخدم كتابة قيمة جديدة في الحقل دون أن يرى قيمته الحالية.
- و**مع** المنحة، تظل القيمة تظهر `****` افتراضيًا. ولكشفها، يفتح المستخدم عنصر **الكشف** في الشريط العلوي، ويختار مدة الكشف – 2 أو 5 أو 10 أو 30 أو 60 دقيقة، أو 3 أو 4 أو 6 أو 8 ساعات – ويعيد التحقق من هويته برمز يُرسل إلى بريده الإلكتروني أو هاتفه، أو برمز من تطبيق المصادقة لديه. وإن لم تتوفر لحسابه أي وسيلة تحقق وكانت مؤسستك قد فعّلت استخدام كلمة المرور بديلًا، يؤكد كلمة مرور حسابه بدلًا من ذلك.
- وما دامت تلك الجلسة نشطة، تظهر قيمة كل حقل حسّاس مُنح المستخدم إذنًا عليه. وترتبط الجلسة بتسجيل الدخول المحدّد ذاك: فعند تسجيل الخروج أو فتح التطبيق على جهاز آخر، تعود القيم إلى الظهور محجوبة هناك، حتى للشخص نفسه. ويُنهي **إلغاء الكشف** الجلسة مبكرًا، وإلا فإنها تنقضي تلقائيًا عند انتهاء المدة المختارة.
- وتُسجَّل في سجل التدقيق عملية تفعيل الجلسة وإلغائها وكل كشف فعلي لقيمة، وبذلك تخضع المنحة للمساءلة وتظل قابلة للسحب.

وإذا أخبرك مستخدم لديه منحة بأنه «لا يملك وصولًا»، فالأرجح أنه لم يبدأ جلسة كشف بعد.

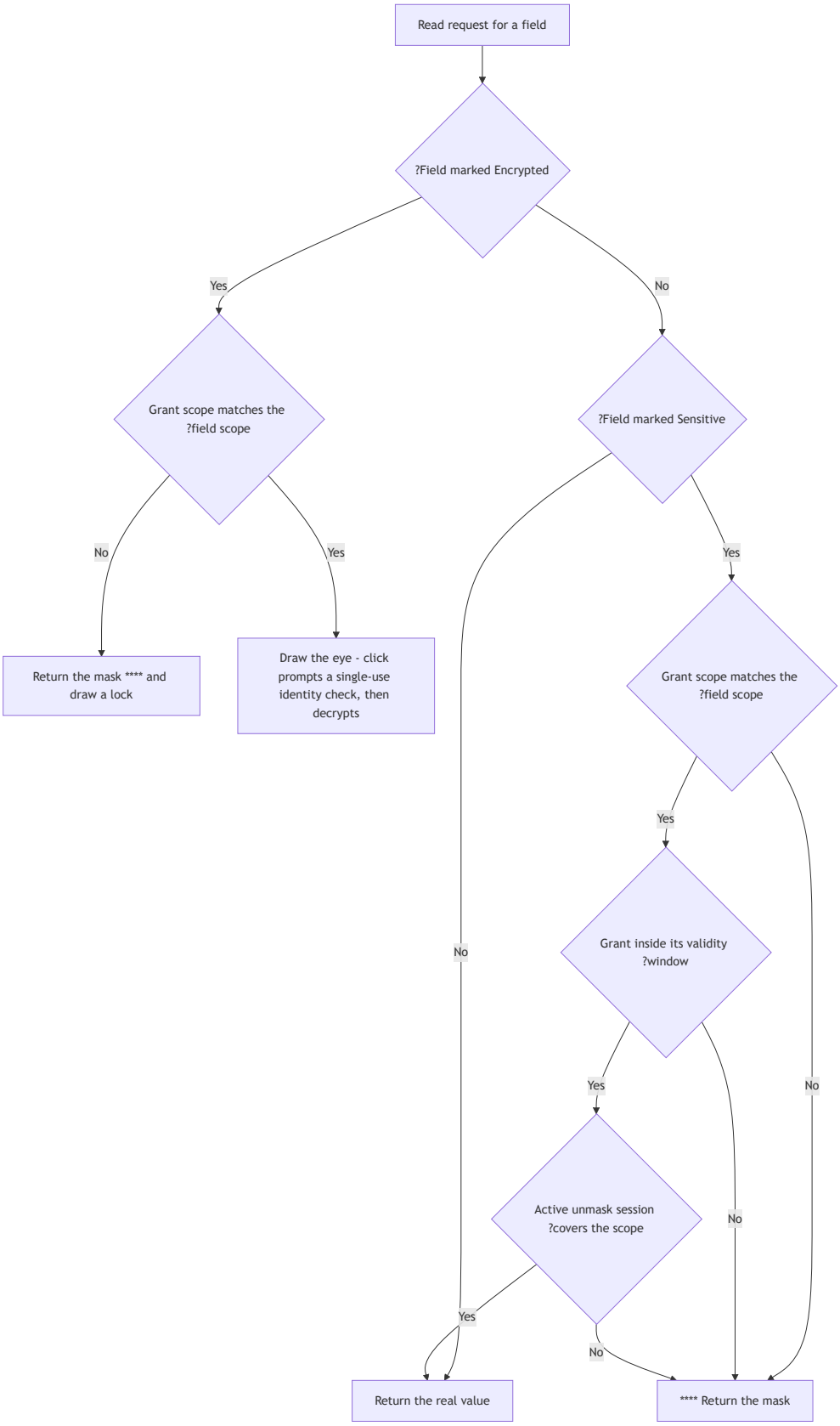
`Since 1.10` **والأيقونة المجاورة للحقل تبيّن له أيّ هذه الحالات هو فيها.** فالقفل يعني *لا منحة إطلاقًا*؛ فلا شيء يمكن النقر عليه، إذ يتعمّد التطبيق ألّا يتيح كشفًا سيضطر إلى رفضه. أما العين فتعني *أنك تحمل منحة*: انقر عليها لتبدأ الكشف. ويسري ذلك على الحقول **المشفَّرة** أيضًا، فمنح الإذن على أحدها أو إبطاله يغيّر الأيقونة الظاهرة لذلك الشخص.

`Since 1.10` **وعلى الحقل المشفَّر، تطلب العين من المستخدم إثبات هويته قبل كشف القيمة**، بالوسائل نفسها المستخدمة في الكشف التقليدي: رمز من تطبيق المصادقة، أو رمز عبر رسالة نصية أو بريد إلكتروني، أو مفتاح مرور، أو كلمة المرور بديلًا. وخلافًا لجلسة **الكشف** التقليدية أعلاه، فإن هذا التحقق أحادي الاستخدام وقصير الأمد (نحو دقيقتين)؛ فلا تختار له مدة، ولا يبدأ جلسة مستمرة تكشف كل حقل حسّاس مُنح الشخص إذنًا عليه، بل يجري التحقق مرة واحدة وتظهر تلك القيمة وحدها. وتبقى القيمة ظاهرة ما دام ذلك الحقل على الشاشة فقط؛ فالانتقال إلى موضع آخر، أو تمرير الحقل خارج نطاق الرؤية، أو تحديث الصفحة، كلها تعيد إخفاءها، ويتطلّب الكشف التالي التحقق من جديد. ويُسجَّل كل كشف ناجح في سجل التدقيق – باسم *فك تشفير*، وهو حدث مستقل عن أحداث الكشف أعلاه – ولا تُكتب القيمة نفسها هناك أبدًا. كما يُسجَّل كل تحقق إضافي (ناجحًا كان أو فاشلًا) بوصفه حدثَ تدقيق مستقلًا. لذا وضّح للمستخدم ما يمكنه توقّعه وفقًا لذلك: تظل المنحة الأساس في تحديد *من يمكنه أصلًا* كشف الحقل، لكن يُطلب من حاملها إثبات هويته في كل مرة، بالصرامة نفسها المتّبعة مع الحقل الحسّاس.

كيف تقرّر المنصة

تُطبّق المنصة قواعد القرار نفسها عند كل قراءة لحقل حسّاس، لكل قارئ ولكل حقل. وباختصار: غياب المنحة، أو وجود منحة خارج فترة صلاحيتها، يعني دائمًا `****`؛ والمنحة على حقل حسّاس تتطلّب كذلك جلسة كشف نشطة؛ والمنحة على حقل مشفَّر تتطلّب كذلك تحققًا من الهوية أحادي الاستخدام لكل كشف.

تفاصيل تقنية: مخطط القرار



وأي فرع يتعذّر حسمه – كتعذّر إجراء استعلام الأذونات، أو عدم توفر مخزن الجلسات – ينتهي بإظهار القيمة محجوبة. فالمنصة تتعمّد حجبها عند حدوث إخفاق في هذا المسار.

صفحات ذات صلة

- الأذونات والوصول – سلّم الصلاحيات على مستوى الكائن الذي تقف هذه المنح إلى جانبه.
- المجموعات – إدارة المجموعات التي تمنحها أذونات حسّاسة.
- المستخدمون – حيث تجد تبويب الحقول الحسّاسة لمستخدم واحد.
- أمان الحساب وكشف البيانات الحساسة [استخدام أسس › أمان الحساب وكشف القيم المحمية] – استخدام المنحة من منظور المستخدم النهائي: طرق التحقق ومعالج الكشف الذي يستخدمه حامل المنحة لكشف قيمة.
- المراقبة: السجلات والتدقيق – حيث تُسجَّل أحداث جلسات الكشف وعمليات الكشف.

التفويض

هذا الدليل موجّه إلى مسؤولي القاطن. يتيح التفويض لشخص أن يعمل نيابةً عن زميل له مدةً محددة، غالبًا لتغطية عمله في أثناء إجازته. ستتعلّم هنا كيف تنشئ تفويضًا، وتقصره على العمل الذي يحتاج إلى تغطية فقط، ثم تُنهيه.

مثال: سارة، مديرة الموارد البشرية، في إجازة مدتها أسبوعان. ينبغي لنائبها كريم أن يعتمد طلبات الإجازة بدلًا منها، دون أن يطّلع على تقارير الرواتب.

كيف يعمل

يحدّد التفويض شخصين ومدةً:

- **المفوض**، أي الشخص الذي تُغطّى مهامه (سارة)،
- و**المفوض له**، أي الشخص الذي يؤدي العمل (كريم)،
- و**من تاريخ**، و**إلى تاريخ** اختياريًا.

ما دام التفويض ساريًا، يستطيع كريم الانتقال من حسابه إلى حساب سارة والعمل بصفتها: يطّلع على بياناتها، ويعبّئ مُدخلاتها ويعدّلها، ويضيف التعليقات، ويعتمد الطلبات أو يقدّمها في سير العمل الخاص بها. ويُنجَز كل ما يفعله باسم سارة، ويسجّل أسس إلى جانب ذلك أن كريم هو من نفّذه فعلًا. ولا يحتاج إلى كلمة مرورها أبدًا.

ولا يمكن أن يحصل كريم على أذونات تتجاوز أذونات سارة، وأنت من يحدّد ما يحصل عليه منها عبر **نطاق** التفويض:

الأساس	ما يحصل عليه كريم	متى تستخدمه
السماح للكل	كل ما تستطيع سارة فعله، باستثناء العناصر التي تُدرجها في **ماعدا**.	حين يغطّي كريم كل شيء تقريبًا. أدرِج العناصر القليلة التي يجب ألا يصل إليها.
منع الكل	لا شيء، باستثناء العناصر التي تُدرجها في **ماعدا**.	حين يغطّي كريم أمرًا واحدًا أو أمرين محددين. أدرِج ما يحتاج إليه تحديدًا.

أما صلاحيات الإدارة فمستقلة؛ إذ لا يحصل كريم على صلاحيات سارة في **الإدارة** إلا إذا سمحت بذلك صراحةً.

قبل أن تبدأ

- يجب أن يكون لكلٍّ من الشخصين حساب مستخدم نشط.
- حدّد مسبقًا ما سيغطّيه المفوَّض له: أيّ الخدمات (تقديم الطلبات، أو الاطلاع على الطلبات، أو صندوق الوارد)، وأيّ المعارض والصفحات والتقارير.
- لا يمكنك أن تُدرج في قائمة **ماعدا** إلا ما تستطيع أنت الوصول إليه. راجع معلومات مفيدة.

إنشاء تفويض

مثال: يتولى كريم اعتماد طلبات الإجازة نيابةً عن سارة مدة أسبوعين، ولا شيء غيرها.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **التفويض**. لا تبدأ من تبويب **التفويض** في سجلّ المستخدم الخاص بالمُفوِّض (سارة)؛ ففي هذا التبويب، يُملأ حقل **المُفوِّض** باسمك أنت (بصفتك مسؤول النظام الذي سجّل الدخول)، ولا يمكنك تغييره.

2. أضِف تفويضًا جديدًا.
3. املأ بيانات الشخصين:
   - **المفوض**: سارة.
   - **المفوض له**: كريم.
4. حدّد المدة:
   - **من تاريخ**: الوقت الذي يبدأ فيه كريم العمل نيابةً عن سارة.
   - **إلى تاريخ**: الوقت الذي ينتهي فيه التفويض. اتركه فارغًا إن أردت تفويضًا بلا تاريخ انتهاء، فيستمر حينئذٍ إلى أن تُنهيه أنت.
   - **نشط**: **نشط**.
5. في **نطاق التفويض**، اضبط **أساس التفويض** على **منع الكل**.
6. في **ماعدا**، اختر صندوق الوارد الخاص بخدمة طلبات الإجازة، كي يتمكّن كريم من معالجة طلبات الإجازة التي تنتظر إجراءً من سارة. راجع اختيار ما يشمله التفويض.
7. اترك **الإدارة** فارغًا ما لم يكن على كريم أن يتولى أعمال سارة الإدارية أيضًا. راجع صلاحيات الإدارة.
8. فعّل، إن شئت، **حول الإشعارات** و**حول البريد الالكتروني**. راجع تحويل الإشعارات ورسائل البريد.
9. اختر **حفظ**.

يبدأ سريان التفويض في الموعد المحدد في **من تاريخ**.

اختيار ما يشمله التفويض

قائمة **ماعدا** شجرةٌ تضم كل ما يمكن تفويضه:

- **التطبيقات**: المعارض والصفحات والتقارير، مجمّعةً حسب الوحدة. (لا يمكن تفويض التقارير إلا على الويب.)
- **الخدمات**: لكل خدمة ثلاثة أجزاء منفصلة يمكنك اختيار كل منها على حدة أو اختيارها معًا:
  - تقديم طلبات جديدة،
  - الاطلاع على الطلبات،
  - صندوق الوارد، أي الطلبات التي تنتظر إجراءً من المُفوَّض.

ويتوقف أثر الاختيار من الشجرة على قيمة **أساس التفويض**:

- مع **السماح للكل**، **يُستثنى** كل ما تختاره. مثال: «السماح للكل» مع اختيار وحدة *تقارير الرواتب* يتيح لكريم أن يفعل كل ما تفعله سارة، باستثناء فتح تقارير الرواتب.
- مع **منع الكل**، **يُشمل** كل ما تختاره، ولا شيء غيره. مثال: «منع الكل» مع اختيار صندوق الوارد الخاص بخدمة طلبات الإجازة يتيح لكريم معالجة طلبات الإجازة التي تنتظر إجراءً من سارة فقط.

وتخضع قوائم **الوارد** و**الصادر** و**المتابعة** لدى كريم، وكذلك دليل الخدمات، للنطاق نفسه ما دام يعمل نيابةً عن سارة، فلا تعرض إلا الخدمات التي يشملها التفويض.

صلاحيات الإدارة

يحدّد خيار **الإدارة** في **نطاق التفويض** ما إذا كان كريم سيحصل أيضًا على صلاحيات سارة في **الإدارة**:

- **مسموح**: يحصل كريم على جميع صلاحيات سارة الإدارية، بما في ذلك مستوى «إدارة» إن كانت تملكه.
- **غير مسموح** (فارغ)، مع **السماح للكل** ومن دون استثناءات: يحتفظ كريم بصلاحيات سارة على مستوى النظام فيما دون مستوى «إدارة»، من دون مستوى «إدارة» نفسه. `Since 1.10`
- **غير مسموح**، مع **منع الكل**، أو مع أي استثناءات: لا يحصل كريم على أيٍّ من صلاحيات سارة على مستوى النظام.

لا تسمح بالإدارة إلا إذا كانت التغطية تتطلّبها فعلًا. ولسحبها لاحقًا، عدّل التفويض وأفرِغ **الإدارة**. ويمكنك أيضًا إزالتها من **الإدارة › إدارة الوصول › أذونات وصول المستخدم**؛ إذ تظهر هناك أذونات كريم الإدارية الموروثة عبر التفويض بالوصف **إذن موروثة من التفويض**.

تحويل الإشعارات ورسائل البريد `Since 1.10`

يكون كلٌّ من **حول الإشعارات** و**حول البريد الالكتروني** معطّلًا افتراضيًا. فعّلهما حين يحتاج المفوَّض له إلى تلقّي ما يُرسَل إلى المُفوِّض أيضًا، كما هو معتاد عند تغطية العمل في الإجازات.

ما الذي يُحوَّل

ما دام التفويض ساريًا، يتلقى المفوَّض له نسخةً من الإشعارات ورسائل البريد التي ترسلها عمليات الأتمتة إلى المُفوِّض، ومن رسائل التقارير المجدولة، وذلك للعمل الذي يشمله التفويض فقط:

- مع **السماح للكل**، تُرسَل النسخة ما لم تكن خدمة الرسالة أو وحدتها أو تقريرها أو معرضها ضمن العناصر المستثناة في **ماعدا**.
- مع **منع الكل**، لا تُرسَل النسخة إلا إذا كانت خدمة الرسالة أو وحدتها أو تقريرها أو معرضها (أو أحد معارض الكيان) ضمن العناصر المشمولة في **ماعدا**. أما الرسالة المتعلقة بمعرض محدد فتتطلّب أن يكون ذلك المعرض نفسه مشمولًا.

ما يتلقاه المفوَّض له:

- **الإشعارات**: نسخة مستقلة غير مقروءة تُبيّن صاحبها. وعند فتحها يُعرض عليه الانتقال إلى حساب المُفوِّض (أو تُفتح مباشرةً إن كان يعمل نيابةً عنه بالفعل). وبعد انتهاء التفويض تظهر النسخة على أنها لم تعد متاحة. وتحمل الإشعارات الفورية العلامة نفسها.
- **رسائل البريد**: يُضاف المفوَّض له في **نسخة إلى** حين يكون المُفوِّض مستلمًا في «إلى» أو «نسخة إلى»، وفي **نسخة مخفية الوجهة** حين يكون المُفوِّض مستلمًا في «نسخة مخفية الوجهة». ولا يُضاف أحد مرتين، ويظل المُفوِّض يتلقى الرسالة.

لا تُرسَل نسخة إلى مفوَّض له معطَّل، ولا إلى المُفوِّض نفسه، ولا – في حالة الإشعارات – إلى مفوَّض له يتلقى الرسالة نفسها مباشرةً. ولا تُحوَّل النسخة مرة أخرى أبدًا. وإذا تعذّر التحويل لأي سبب، تُسلَّم الرسالة الأصلية مع ذلك.

راجع أيضًا إعداد الإشعارات.

متى يكون التفويض ساريًا

لا يعمل التفويض إلا ما دامت جميع الشروط التالية متحققة:

1. قيمة **نشط** هي **نشط**.
2. حلّ الموعد المحدد في **من تاريخ**.
3. **إلى تاريخ** فارغ أو لم يحلّ موعده بعد.

4. لم يُؤرشَف التفويض.

وإذا تعدّدت التفويضات من المُفوِّض نفسه إلى الشخص نفسه، فلا يرى المفوَّض له ذلك المُفوِّض إلا مرة واحدة.

إنهاء التفويض

ينتهي التفويض تلقائيًا في الموعد المحدد في **إلى تاريخ**. ولإنهاء تفويض قبل موعده، أو لإنهاء تفويض بلا تاريخ انتهاء، افتحه ونفّذ أحد الإجراءات التالية:

- اضبط **إلى تاريخ** على الوقت الحالي، أو
- اضبط **نشط** على **غير نشط**، أو
- أرشِف التفويض.

يسري التغيير على الإجراء التالي الذي يتخذه المفوَّض له. فعند حلول الموعد المحدد في **إلى تاريخ**، يُعاد المفوَّض له الذي لا يزال يعمل بصفة المُفوِّض إلى حسابه الخاص. أما عند ضبط **غير نشط** أو أرشفة التفويض، فيفقد إمكانية الوصول إلى ما لدى المُفوِّض.

وعندما يغادر المُفوِّض أو المفوَّض له المؤسسة، أنهِ جميع تفويضاته. راجع إنهاء خدمة شخص يغادر.

ما يراه المفوَّض له

قد تحتاج إلى شرح ما يلي للشخص الذي يتولى التغطية:

1. يفتح قائمته الشخصية (صورته أو اسمه في أعلى الشاشة)، فيجد قسم **التفويضات** الذي يسرد أسماء كل من فوّضه.
2. يختار اسم المُفوِّض، فينقله أسس إلى حساب المُفوِّض، ويظهر في أعلى الشاشة اسمه هو، ثم سهم، ثم اسم المُفوِّض، فيتّضح دائمًا باسم من يعمل.
3. للعودة إلى حسابه الخاص، يختار **خروج**.

ويُنهي تسجيل الخروج على الويب كذلك العمل بموجب التفويض الحالي، ليعود عند تسجيل الدخول التالي إلى حسابه الخاص. `Since 1.6` أما على الهاتف المحمول، فيؤدي اختيار تفويض إلى إعادة تحميل التطبيق بصفة المُفوِّض.

لا يستطيع العمل بموجب التفويض إلا الشخص المذكور في **المفوض له**، ولا يمكن لأي شخص آخر استخدامه، حتى لو كان لديه رابط إليه. `Since 1.6`

معلومات مفيدة

- **قائمة «ماعدا» تعرض ما تستطيع الوصول إليه.** `Since 1.8` إذا كان لديك مستوى صلاحية على النظام (عرض أو مطوّر أو تعديل أو إدارة)، تعرض القائمة كل وحدة ومعرض وصفحة وتقرير وخدمة منشورة، وإلا فلا تعرض إلا ما تستطيع أنت الوصول إليه. ويحدّ هذا مما تستطيع اختياره فحسب؛ فالمفوَّض له لا يحصل أبدًا على أذونات تتجاوز أذونات المُفوِّض، أيًّا كان ما تختاره.
- **تصل التغييرات إلى المفوَّض له فورًا.** فتعديل التفويض أو أرشفته، أو تغيير أذونات المُفوِّض نفسه، يسري على الإجراء التالي الذي يتخذه المفوَّض له.
- **سجل التدقيق.** يُسجَّل كل إجراء يُتخذ بموجب تفويض باسم المُفوِّض، مع بيان المفوَّض له الذي نفّذه فعلًا، بما في ذلك النقرات على الأزرار في سجل المُدخل. راجع المراقبة: السجلات والتدقيق.

- **التفويض مخصّص للأشخاص.** وإذا أردت أن يعمل نظام خارجي في أسس، فأنشئ مستخدم تطبيق بدلًا من ذلك. راجع مستخدمو التطبيقات.
- **الزوار الذين لم يسجّلوا الدخول** لا تفويضات لهم.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
لا يرى المفوَّض له المُفوِّض ضمن **التفويضات**.	تحقّق من الشروط الأربعة في متى يكون التفويض ساريًا، ولا سيما **نشط** والتاريخين.
يُعاد المفوَّض له فجأة إلى حسابه الخاص.	انتهى التفويض، أو لم يبدأ بعد. تحقّق من **من تاريخ** و**إلى تاريخ**.
يستطيع المفوَّض له الانتقال إلى الحساب لكنه لا يرى شيئًا.	مع **منع الكل**، لا يُشمل إلا ما في **ماعدا**. أضِف المعارض أو الصفحات أو الخدمات التي يحتاج إليها.
يستطيع المفوَّض له أن يفعل أكثر مما ينبغي.	مع **السماح للكل**، يُشمل كل ما لم يُستثنَ. انتقل إلى **منع الكل**، أو أضِف استثناءات، وتحقّق من **الإدارة**.
يرى المفوَّض له، أثناء العمل نيابةً عن المُفوِّض، عددًا بجانب **الوارد**، لكن القائمة فارغة.	هذه مشكلة معروفة في المنتج، ولم يُؤكَّد بعد أي حل بديل لها.
لا يتلقى المفوَّض له أي إشعارات أو رسائل بريد محوّلة.	فعّل **حول الإشعارات** / **حول البريد الالكتروني**، وتحقّق من أن خدمة الرسالة أو تقريرها ضمن النطاق.

للتعمّق أكثر

لمطوّري التكامل: واجهة الـ API للتفويض وآلية فرضه [التكامل والتوسعة › واجهة التفويض البرمجية وآلية فرضه] · للمشغّلين: عمليات البوابة: user-delegation

إعدادات المنظمة

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتبيّن لك كيفية ضبط الإعدادات الافتراضية لكل من في مؤسستك – اللغة والمنطقة الزمنية وصيغ التاريخ – وإضافة لغة أو منطقة زمنية، وربط واتساب. كما تشرح عناصر هوية مؤسستك، مثل اسم المنتج والشعار، التي يضبطها المشغّل بدلًا من ضبطها في **الإدارة**.

وللسمات والخطوط والأيقونات صفحة خاصة: المظهر.

كيف تعمل

يجمع **مُدخل الإعدادات** الخيارات التي تحدّد ما يظهر للمستخدمين: السمات المتاحة والسمة الافتراضية، واللغة الأولى، والمنطقة الزمنية، وصيغ التاريخ والوقت. وينطبق كل مُدخل على **نطاق** واحد:

النطاق	على من ينطبق
المنظمة	كل من في مؤسستك، وهو الأساس الذي تبدأ به.
المساحة	كل من يعمل في مساحة واحدة.
المستخدم	شخص واحد.

وعندما تنطبق عدة مُدخلات، يُعتمد أكثرها تحديدًا: مُدخل الشخص نفسه، ثم مُدخل مساحته، ثم مُدخل المنظمة. أما الزوار الذين لم يسجّلوا الدخول فلا يُطبَّق عليهم إلا مُدخل المساحة؛ فإن لم يكن للمساحة مُدخل، استُخدمت الإعدادات الافتراضية المدمجة، لا مُدخل المنظمة.

مثال. تستخدم مؤسستك الإنجليزية وتعرض التواريخ بدءًا باليوم. وتخدم مساحة الموارد البشرية فريقًا ناطقًا بالعربية، لذا يكون لها مُدخل إعدادات خاص تكون فيه العربية اللغة الأولى. ويُخصَّص لمديرة موارد بشرية تعمل مع مكتب لندن مُدخل شخصي يستخدم المنطقة الزمنية للندن. أما الباقون فيحتفظون بالإعدادات الافتراضية للمنظمة.

أدِر كل ذلك ضمن **الإدارة › الواجهات**، التي تضم شاشات **اللغات** و**المناطق الزمنية** و**الإعدادات** المستخدمة في هذه الصفحة (إضافةً إلى **السمات** و**الخطوط**، الموضّحتين في المظهر، و**القوالب**، الموضّحة في إعداد الإشعارات). وتظهر **الواجهات** في القائمة لمن لديه مستوى وصول **مطور** على الأقل على مستوى النظام، أما إضافة المُدخلات أو تغييرها فتتطلب مستوى **تعديل**. راجع الأذونات والوصول.

ضبط الإعدادات الافتراضية لمنظمتك

1. افتح **الإدارة › الواجهات › الإعدادات**، ثم اختر **إضافة ضبط**.
2. في **النطاق**، اختر **المنظمة** أو **المساحة** أو **المستخدم**، ليظهر حقل تختار منه المنظمة أو المساحة أو الشخص.
3. اختر المظهر والصيغ:
   - **السمات المتاحة** – السمات التي يستطيع المستخدمون التبديل بينها.
   - **السمة الافتراضية** – السمة التي تظهر للمستخدمين إلى أن يختاروا غيرها.
   - **اللغة الأولى** – اللغة الافتراضية، وتُعرض برمزها، مثل `ar` أو `en`.
   - **المنطقة الزمنية** – المنطقة الزمنية التي تُعرض وفقها التواريخ والأوقات.
   - **تنسيق الوقت والتاريخ** و**تنسيق التاريخ** و**تنسيق الوقت** – طريقة كتابة التواريخ والأوقات.

4. اختر **حفظ**.

ابدأ بمُدخل واحد من نوع **المنظمة**، ولا تُضف مُدخلات من نوع **المساحة** أو **المستخدم** إلا عند وجود حاجة فعلية إلى إعدادات مختلفة. ولا يمكن أن يكون لكل مساحة أو لكل شخص أكثر من مُدخل إعدادات واحد.

ولتغيير إعداد افتراضي لاحقًا، افتح المُدخل من قائمة **الإعدادات**، وعدّله، ثم احفظه. ويسري التغيير في المرة التالية التي يحمّل فيها المستخدمون التطبيق.

> ⚠ **مشكلة معروفة: لا تعرض قائمة الإعدادات إلا مُدخل المنظمة**
>
> تُفتح قائمة **الإعدادات** بمرشِّح **النطاق** الذي لا يعرض إلا مُدخل **المنظمة**. وتظل مُدخلات **المساحة** و**المستخدم** سارية، لكنها لا تظهر في القائمة، وقد لا تظهر حتى بعد مسح المرشِّح؛ لذا قد لا تتمكن من فتح أحدها من القائمة لتغييره أو أرشفته. وهذه مشكلة معروفة في المنتج.

> 🚀 **السمة الافتراضية متاحة دائمًا**
>
> لا يلزمك إدراج السمة الافتراضية ضمن **السمات المتاحة** أيضًا، فهي متاحة دائمًا. وإذا لم ينطبق أي مُدخل إعدادات على شخص ما، استُخدمت له السمة الافتراضية المدمجة.

إضافة لغة

يخزّن أسس كل اسم وتسمية بكل لغة من لغاتك، لذا تتيح إضافة لغة للمستخدمين العمل بها في كل مكان.

1. افتح **الإدارة › الواجهات › اللغات**، ثم اختر **إضافة لغة**.
2. املأ النموذج:
   - **اسم اللغة** – اسم اللغة كما يكتبه الناطقون بها، مثل *Français*.
   - **العلم** – العلم الذي يظهر بجانبها.
   - **رمز اللغة** – الرمز المكوّن من حرفين، مثل `fr`. ولكل لغة رمزها الخاص.
   - **الإتجاه** – **من اليسار الى اليمين** أو **من اليمين إلى اليسار**.
   - **افتراضي** – فعّله للغة الوحيدة التي تريد اعتمادها لغةً افتراضية.
   - **ملفات الترجمة للويب** و**ملف الترجمة للموبايل** – ترجمات تسميات المنتج نفسه في تطبيق الويب وتطبيق الهاتف المحمول.
3. اختر **حفظ**.

فعّل **افتراضي** للغة واحدة فقط.

> ⚠ **حذف لغة أو إعادة تسميتها يترك فراغات**
>
> إذا حذفت لغة أو أعدت تسميتها، تظل الأسماء والتسميات التي كُتبت بها فارغة لتلك اللغة، ولا يملؤها أسس نيابةً عنك. لذا راجع بعد ذلك مُدخلاتك ومعارضك وخدماتك المهمة، واملأ الأسماء الناقصة.

تفاصيل تقنية

تقرأ المنصة قائمة اللغات عند بدء تشغيل خدماتها، لذا قد لا تظهر اللغة المضافة حديثًا في كل مكان إلى أن يعيد المشغّل تشغيل الخدمات. وإذا لم تُحدَّد أي لغة بوصفها الافتراضية، تختار المنصة لغة نيابةً عنك، لذا حدّد اللغة الافتراضية بنفسك دائمًا.

إضافة منطقة زمنية

1. افتح **الإدارة › الواجهات › المناطق الزمنية**، ثم اختر **إضافة منطقة زمنية**.
2. املأ **المنطقة الزمنية** (اسمها)، و**رقم المنطقة**، و**الفرق الزمني** (الإزاحة عن UTC)، و**التوقيت الشتوي** إن كان ينطبق.
3. اختر **حفظ**.

يمكنك بعد ذلك اختيار المنطقة الزمنية الجديدة في مُدخل إعدادات. وتؤثر المناطق الزمنية في المواعيد النهائية أيضًا؛ إذ تُحتسب المهل الزمنية في سير العمل بساعات العمل، وفق المنطقة الزمنية المعتمدة. راجع ساعات العمل ومراقبة الوقت.

ربط واتساب `Since 1.10`

يستطيع أسس إرسال رسائل واتساب من رقم واتساب للأعمال الخاص بمؤسستك: رسائل من عمليات الأتمتة، ورموز تسجيل الدخول. وتربط رقمك في **إعدادات النظام**.

كيف يعمل. تضم إعدادات النظام مُدخلًا واحدًا على مستوى المنظمة ينطبق على كل المساحات، ويمكن أن تضم مُدخلًا إضافيًا لكل مساحة. وتستخدم المساحة التي لها بيانات واتساب خاصة بها بياناتها وحدها، ولا تخلطها ببيانات المنظمة.

> **لا توجد شاشة مخصّصة بعد**
>
> لا توجد في الإصدار 1.10 شاشة لإعدادات النظام، لذا عدّل مُدخلاتها كما تعدّل المُدخلات العادية، على النحو الموضح أدناه.

قبل أن تبدأ

اطلب ممن يدير حساب WhatsApp Business الخاص بشركتك في Meta ما يلي:

- **معرف رقم الهاتف** و**معرف حساب الأعمال** للرقم الذي ستُرسل منه الرسائل؛
- **رمز الوصول** و**سر التطبيق** الخاص بتطبيق Meta؛
- لرموز تسجيل الدخول، اسم **قالب رسالة معتمد لرموز تسجيل الدخول** ولغته.

واختر كذلك **رمز التحقق من الويب هوك**، وهو عبارة سرية ستُدخلها هنا وفي Meta.

ربط رقمك

1. تأكد من أنك تعمل في المساحة الرئيسية (الافتراضية) لمنظمتك، إذ لا يمكنك تغيير المُدخل الخاص بالمنظمة كلها إلا من هناك.
2. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **إعدادات النظام**.
3. افتح المُدخل الذي لم يُحدَّد فيه حقل **المساحة**، فهذا هو المُدخل الخاص بالمنظمة كلها.

4. اختر **تعديل** واملأ قسم **واتساب**:

الحقل	ما الذي تُدخله
المزود	اتركه على Meta، فهو المزوّد الوحيد.
معرف رقم الهاتف	معرّف الرقم الذي تُرسل منه الرسائل.
معرف حساب الأعمال	معرّف حساب WhatsApp Business الخاص بك، ويُستخدم لعرض قائمة قوالبك المعتمدة.
رمز الوصول	رمز الوصول من Meta.
رمز التحقق من الويب هوك	العبارة السرية التي اخترتها.
سر التطبيق	سر تطبيق Meta.
قنوات رمز التحقق المسموحة	القنوات المسموح بإرسال رموز تسجيل الدخول عبرها: رسالة نصية، أو واتساب، أو كلاهما. واستبعد واتساب إن كنت لا تريد إرسال رموز تسجيل الدخول عبره.
قناة رمز التحقق الافتراضية	القناة التي تُعرض أولًا حين تتاح القناتان.
اسم قالب رمز التحقق و**لغة قالب رمز التحقق**	قالب رموز تسجيل الدخول المعتمد لديك ولغته.

5. اختر **حفظ**.

6. في تطبيق Meta الخاص بك، سجّل الويب هوك الخاص بحالة التسليم، ليُظهر سجل الرسائل ما إذا كانت الرسائل قد سُلّمت وقُرئت. واطلب من المشغّل عنوان الويب هوك الخاص بمساحتك، وأدخل فيه رمز التحقق من الويب هوك الخاص بك.

7. اطلب من المشغّل تفعيل الإرسال الفعلي عبر واتساب لمؤسستك. وإلى أن يفعّل الإرسال، لا تُرسل أي رسالة، وتظهر كل رسالة بالحالة **لم تُرسل (الإرسال معطل)** في سجل الرسائل.

ولتخصيص رقم لمساحة واحدة، أضِف مُدخلًا في إعدادات النظام، وحدّد **المساحة** الخاصة به، واملأ كل حقل من حقول واتساب تحتاج إليه تلك المساحة.

معلومات مفيدة

- **يتطلب الإرسال معرّف رقم الهاتف ورمز الوصول.** كما تتطلب رموز تسجيل الدخول عبر واتساب إدراج واتساب ضمن **قنوات رمز التحقق المسموحة** وتحديد قالب لرموز تسجيل الدخول.
- **تؤثر رموز تسجيل الدخول عبر واتساب في كل من لديه رقم هاتف موثّق.** فبمجرد إعدادها، يُطلب من أصحاب أرقام الهواتف الموثّقة إدخال رمز عند تسجيل الدخول. اقرأ رموز واتساب قبل أن تضيف واتساب إلى **قنوات رمز التحقق المسموحة**.
- **تبقى الأسرار مخفية.** فبعد الحفظ، لا يظهر لرمز الوصول وسر التطبيق ورمز التحقق من الويب هوك سوى حالة كل منها: مضبوط أو غير مضبوط.
- **تسري التغييرات فورًا** على الرسالة التالية التي تُرسل.
- **رقم واحد، مُدخل واحد.** لا يمكن استخدام معرّف رقم الهاتف إلا في مُدخل نشط واحد على مستوى منظمتك كلها.
- **لا يمكن أرشفة المُدخل الخاص بالمنظمة كلها.** أما مُدخل المساحة فيمكن أرشفته.
- **يجب أن تشمل رخصتك الإدارة.** فتغيير إعدادات النظام يتطلب ذلك. راجع رخصتك.

للتعرّف على مواضع استخدام واتساب بعد ذلك، راجع قناة واتساب، وسجل رسائل واتساب، ورموز تسجيل الدخول عبر واتساب. ويرسل بُناة التطبيقات رسائل واتساب من عمليات الأتمتة؛ راجع التفاعلات والأتمتة [بناء التطبيقات].

اسم منظمتك وشعارها وصفحة تسجيل الدخول

اسم المنتج والشعار وأيقونة الموقع والسمة الأساسية التي يراها المستخدمون في تطبيق الويب وفي صفحة تسجيل الدخول **لا** تُضبط في **الإدارة**. بل تُحدَّد في إعدادات النشر لديكم، وفي النشر المشترك تُستمدّ من **العلامة التجارية** لمؤسستك: أي مجموعة الاسم والشعارات والسمة وعنوان مرسِل البريد الإلكتروني التي سُجّلت بها مؤسستك. `Since 1.10`

تظهر العلامة التجارية في:

- تطبيق الويب: اسم المنتج، والشعارات، وأيقونة الموقع، والسمة، وشاشة التحميل؛
- صفحات تسجيل الدخول، ورسائل رموز تسجيل الدخول، والاسم الذي يظهر في تطبيقات المصادقة؛
- رسائل البريد التي لا تحدّد مرسِلًا خاصًا بها، إذ تُرسل من عنوان العلامة التجارية.

ولتغيير أيٍّ من ذلك، اطلب من المشغّل إجراء التغيير. فالعلامة التجارية للمؤسسة ثابتة بمجرد تسجيلها، ويتطلّب تغييرها أن ينقل المشغّل مؤسستك.

صفحة تسجيل الدخول `Since 1.10`

يضبط المشغّل كذلك مظهر صفحة تسجيل الدخول نفسها: شعارها، وألوانها، وتنسيقها، ورابط **إنشاء حساب** الاختياري، ورسائل البريد التي يتلقاها المستخدمون لتعيين كلمة المرور أو إعادة تعيينها. وقد تلاحظ أمرين:

- **رابط إنشاء الحساب يُبقي صفحة تسجيل الدخول ظاهرة.** فعندما يكون مزوّد دخول موحّد واحد هو الوسيلة الوحيدة لتسجيل الدخول في نطاق ما، ينتقل المستخدمون عادةً مباشرةً إلى ذلك المزوّد. أما إذا هُيّئ رابط إنشاء حساب، فتظهر صفحة تسجيل الدخول بدلًا من ذلك، ليتمكّن المستخدمون من الاختيار. راجع طرق تسجيل الدخول والدخول الموحّد.
- **في صفحة تسجيل الدخول رابط «إلغاء» دائمًا.** ولا يمكن تعطيله.

وإذا تغيّر لون التمييز في صفحة تسجيل الدخول لديكم إلى الأحمر بعد الترقية إلى 1.10، فاطلب من المشغّل تحديد لونكم صراحةً.

العملات

قائمة العملات موحّدة لجميع المؤسسات ولا يمكن تعديلها. وتتاح كل عملة في كل حقل مالي، ويمكن دائمًا لمن يستطيع رؤية حقل مالي أن يرى عملته.

> **للتعمّق أكثر**
>
> للمشغّلين ومطوّري التكامل: إعدادات القاطن والمظهر: مرجع تقني · خادم الهوية

ساعات العمل والعطلات

يوجَّه هذا الدليل إلى مسؤولي القاطن، ويبيّن لك كيفية تعريف **ساعات العمل** و**العطلات** الخاصة بمؤسستك. ويستخدمها بُناة التطبيقات عند تحديد مهلة زمنية لخطوة في سير العمل؛ إذ لا يُحتسب في العدّ التنازلي حينئذٍ إلا وقت العمل، فلا تنقضي مهلة اعتماد مدتها «يومان» خلال عطلة نهاية الأسبوع أو عطلة رسمية.

كيف تعمل

يستطيع باني التطبيقات تحديد مهلة زمنية لأي خطوة في سير العمل، مثل «يجب أن تعتمد الموارد البشرية طلب الإجازة خلال 16 ساعة عمل». ولتحديد المقصود بـ«ساعات العمل»، ترتبط الخطوة بأحد **جداول ساعات العمل** لديك. وحين يصل طلب إلى الخطوة، يحسب أسس موعده النهائي باحتساب الوقت المحدّد في ذلك الجدول فقط، مع استثناء كل يوم مسجّل بوصفه **عطلة**.

مثال. يعمل مكتبك من الأحد إلى الخميس، من 8:00 إلى 16:00. ويصل طلب إجازة إلى الموارد البشرية يوم الخميس الساعة 14:00 بمهلة قدرها 16 ساعة عمل:

- الخميس من 14:00 إلى 16:00: تُحتسب منه ساعتان.
- الجمعة والسبت غير مُدرجين في الجدول، فلا يُحتسب منهما شيء.
- الأحد عطلة رسمية أدخلتها، فلا يُحتسب منه شيء.
- الاثنين من 8:00 إلى 16:00: تُحتسب منه 8 ساعات، ثم الثلاثاء من 8:00 إلى 14:00: تُحتسب منه الساعات الست الأخيرة.

وبذلك يكون الموعد النهائي **الثلاثاء الساعة 14:00**. وإذا لم تتخذ الموارد البشرية إجراءً بحلول هذا الموعد، تصبح الخطوة **متأخرة** (Overdue)، ويبدأ أي تصعيد أعدّه باني التطبيقات.

أنت من يُعدّ الجداول والعطلات؛ أما باني التطبيقات فيحدّد الخطوات التي لها مهل زمنية، ومدد تلك المهل، وما يحدث عند تجاوز إحداها.

قبل أن تبدأ

- تحتاج إلى إذن الوصول إلى **الإدارة › التطبيقات › الكيانات**، إذ تُحفظ ساعات العمل والعطلات هناك بوصفها مُدخلات في كيانَي **ساعات العمل** و**العطلات**.
- حدّد عدد الجداول التي تحتاج إليها: عادةً ما تحتاج إلى جدول واحد لكل نمط عمل مختلف، مثل *ساعات الدوام المكتبي*، و*مكتب الدعم على مدار الساعة*، و*وردية عطلة نهاية الأسبوع في الفرع*.

إنشاء جدول ساعات عمل

مثال: *ساعات الدوام المكتبي*، من الأحد إلى الخميس، من 8:00 إلى 16:00.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **ساعات العمل**.

2. اختر **إضافة ساعات عمل**.

3. أدخل **الاسم** بكل لغة، مثل *ساعات الدوام المكتبي*.

4. ضمن **ساعات العمل**، أضِف صفًا لكل يوم عمل:

   - **اليوم**: مثل *الأحد*.
   - **بداية الوقت**: 8:00.
   - **نهاية الوقت**: 16:00.

   لا يمكن إدراج اليوم الواحد إلا مرة واحدة، ويُعدّ أي يوم ليس له صف يوم عطلة.

5. اختر **حفظ**.

أنشئ جدولًا منفصلًا لكل نمط عمل.

إضافة العطلات

مثال: عيد الفطر، ثلاثة أيام، للجميع.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **العطلات**.
2. اختر **أنشئ مدخل**.
3. أدخل **الاسم**، مثل *عيد الفطر*.
4. في **Start and End Date** (تاريخ البداية والنهاية)، اختر اليوم الأول واليوم الأخير من العطلة. وتشمل العطلة هذين اليومين وجميع الأيام الواقعة بينهما.
5. في **ساعات العمل المرتبطة**، اختر الجداول التي تنطبق عليها العطلة، أو اترك الحقل فارغًا لتطبيق العطلة على **كل** الجداول.
6. اختر **حفظ**.

استخدم **ساعات العمل المرتبطة** حين تنطبق العطلة على بعض الفرق فقط، مثل عطلة يستمر خلالها مكتب الدعم على مدار الساعة في العمل.

تغيير جدول أو عطلة أو إزالتهما

عدّل المُدخل أو أرشِفه كما تفعل مع أي مُدخل آخر. وتسري التغييرات فورًا على كل خطوة يصل إليها طلب بعد إجراء التغيير.

`Since 1.10`

أما الخطوة التي بدأ عدّها التنازلي فتحتفظ بالموعد النهائي الذي حُدّد لها حين وصل إليها الطلب؛ لذا فإن إضافة عطلة اليوم لا تغيّر الموعد النهائي لطلب وصل أمس.

وقبل أن تؤرشف جدولًا، اسأل بُناة التطبيقات عمّا إذا كانت أي خطوة لا تزال تستخدمه؛ إذ لا يُحدَّد موعد نهائي إطلاقًا لخطوة لا يتضمن جدولها أي أيام عمل.

كيف يستخدم بُناة التطبيقات جداولك

فيما يلي الإعدادات التي يضبطها باني التطبيقات للخطوة، لتعرف ما تتوقعه. وتشمل إعدادات **التوقيت** للخطوة ما يلي:

الإعداد	ما يفعله
التوقيت	يفعّل المهلة الزمنية للخطوة.
نظام التوقيت	جدول ساعات العمل الذي تُحتسب المهلة وفقه، وهو أحد جداولك.
وحدة الزمن	**دقائق** أو **ساعات** أو **ثواني**.
آلية حساب الوقت	**قيمة ثابتة** (المهلة نفسها في كل مرة)، أو **قيمة حقل** (مأخوذة من حقل في المُدخل)، أو **تعبير** (محسوبة، كمهلة أقصر للطلبات العاجلة مثلًا).
القيمة / القيمة البديلة حال الفشل	المهلة نفسها، والقيمة المستخدمة حين لا يُرجع الحقل أو التعبير رقمًا.

وتكون حالة كل خطوة مراقَبة **قيد الانتظار** ما دامت تنتظر، و**منجزة في الوقت** (Achieved) حين تُستكمل ضمن المهلة، و**متأخرة** (Overdue) حين يحلّ الموعد النهائي قبل اكتمالها. ويتحقق أسس من المواعيد التي انقضت كل دقيقة؛ لذا قد تتغير حالة الخطوة إلى **متأخرة** بعد موعدها النهائي بما يصل إلى دقيقة.

ويرد شرح إعدادات باني التطبيقات في سير العمل: المهل الزمنية والتصعيد [بناء التطبيقات › سير العمل والاعتمادات].

حين تتأخر خطوة

لا يترتب على تجاوز الموعد النهائي وحده إلا وضع علامة **متأخرة** على الخطوة. ولاتخاذ إجراء عندئذٍ، يضيف باني التطبيقات تفاعلًا إلى الكيان، ضمن قسم **مراقبة الوقت** في تبويب **التفاعلات** الخاص بالكيان، ويختار الحدث **عند تجاوز الوقت المحدد**:

- **أختر الخطوة**: الخطوة التي يراقبها التفاعل.
- **انتظر لمدة**: المدة التي ينتظرها التفاعل بعد الموعد النهائي قبل اتخاذ الإجراء أول مرة، **بالثواني**.
- **كرر كل**: المدة بين كل تكرار والتكرار الذي يليه، **بالثواني**.
- **توقف بعد**: عدد مرات التكرار.
- الإجراء، مثل إشعار مدير مالك الخطوة، أو نقل الخطوة إلى شخص آخر.

وتُحتسب فترات الانتظار من وقت العمل أيضًا، وفق الجدول والعطلات نفسها. ومن أمثلة التصعيد المعتادة: تذكير المالك عند حلول الموعد النهائي، ثم إشعار مديره كل أربع ساعات عمل، ثلاث مرات. ولتفاعل المدير يعني ذلك **انتظر لمدة** 14400 (أربع ساعات بالثواني)، و**كرر كل** 14400، و**توقف بعد** 2: التنفيذ الأول، ثم تكراران.

راجع التفاعلات والأتمتة [بناء التطبيقات].

المناطق الزمنية

ليس للجدول منطقة زمنية خاصة به؛ إذ يتعامل أسس مع **بداية الوقت** و**نهاية الوقت** بوصفهما وقتين خلال اليوم، ويطبّقهما على كل يوم يحتسبه، كما يتعامل مع العطلات بوصفها أيامًا تقويمية كاملة.

بعد إعداد جدولك الأول، تحقّق من موعد نهائي واحد: أرسل طلبًا تجريبيًا عبر خطوة مراقَبة، وقارن موعدها النهائي بما تتوقعه. وإذا كانت المواعيد النهائية تختلف عمّا تتوقعه ببضع ساعات، فاطلب من المشغّل التحقق من المنطقة الزمنية المستخدمة في حساب الوقت في المنصة. راجع محرّك وقت العمل واتفاقيات مستوى الخدمة.

معلومات مفيدة

- **يحتاج كل جدول إلى يوم عمل واحد على الأقل.** فالجدول الخالي من وقت العمل لا يمكن أن يُنتج موعدًا نهائيًا أبدًا.

- **العطلات المؤرشفة لا يُعتدّ بها.**
- **العطلات أيام كاملة.** فلا توجد عطلات نصف يوم.
- **بيانات المهل الزمنية تغذّي التقارير.** إذ يستطيع بُناة التطبيقات إعداد تقارير عن الخطوات التي تأخرت ومواضع تأخرها، لاكتشاف الاختناقات.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
خطوة مراقَبة لا تصبح **متأخرة** أبدًا.	**نظام التوقيت** للخطوة فارغ، أو مؤرشف، أو بلا أيام عمل، أو أن مهلة الخطوة تساوي صفرًا. اطلب من باني التطبيقات التحقق من إعدادات **التوقيت** للخطوة.
يقع موعد نهائي في يوم عطلة.	العطلة غير مرتبطة بذلك الجدول. تحقّق من **ساعات العمل المرتبطة**، أو اترك الحقل فارغًا لتطبيق العطلة على جميع الجداول.
لم تغيّر عطلة جديدة موعدًا نهائيًا.	وصل ذلك الطلب إلى الخطوة قبل أن تضيف العطلة. فالمواعيد النهائية تُثبَّت عند وصول الطلب إلى الخطوة.
المواعيد النهائية تختلف عمّا تتوقعه ببضع ساعات.	راجع المناطق الزمنية.
لا يمكن إيقاف **التوقيت** على خطوة.	هناك تفاعل يستخدمه، ويجب على باني التطبيقات إزالة ذلك التفاعل أو تغييره أولًا.

للتعمّق أكثر

للمشغّلين والمهندسين: محرّك وقت العمل واتفاقيات مستوى الخدمة · لبُناة التطبيقات: سير العمل: المهل الزمنية والتصعيد [بناء التطبيقات › سير العمل والاعتمادات]

المساحات والنطاقات

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتوضّح لك كيفية إنشاء مساحة، وإضافة الأشخاص إليها، ووضعها في وضع الصيانة أو إيقافها، وعلاقة ذلك بعناوين الويب التي يستخدمها الناس، أي النطاقات. ولمعرفة ما يراه الناس عند التنقّل بين المساحات، راجع تسجيل الدخول واختيار مساحة [استخدام أسس].

كيف تعمل

المساحة منطقة عمل مستقلة داخل مؤسستك، لها عنوانها الخاص، وتضم مُدخلاتها وتطبيقاتها ومعارضها وأعضاءها. ولا يرى الناس إلا المساحات التي هم أعضاء فيها، ولا يطّلعون داخل كل مساحة إلا على بياناتها.

النطاق هو عنوان الويب (أو عناوين الويب) الذي يستخدمه الناس لفتح أسس، وما يُتاح فيه من خيارات تسجيل الدخول: كلمات المرور، ومفاتيح المرور، ورموز العامل الثاني، وأزرار الدخول الموحّد.

مثال. تشغّل Contoso منصة أسس على العنوان `contoso.example.com`، وتضم مساحتها الافتراضية التطبيقات المشتركة على مستوى الشركة. وتحصل إدارة الموارد البشرية على مساحة خاصة بها، `hr.contoso.example.com`، تقتصر عضويتها على موظفي الموارد البشرية. وتُتاح خدمة طلبات الإجازة في المساحة الافتراضية، فيستطيع الجميع استخدامها؛ أما تطبيق مراجعة الرواتب فيوجد في مساحة الموارد البشرية، فلا يعلم أحد من خارجها حتى بوجوده.

تبدأ كل منظمة بـ **مساحة افتراضية** واحدة، تُتاح على العنوان الرئيسي، وتضم الإعدادات على مستوى المنظمة، ولا يمكن تعطيلها.

أدِر المساحات من **الإدارة › المساحات**، التي لا تظهر لك إلا إذا كانت لديك صلاحية **إدارة** على مستوى النظام.

إنشاء مساحة

1. افتح **الإدارة › المساحات**، ثم اختر **مساحة جديدة**.
2. املأ النموذج:
   - **النوع** – **مستقل** لمساحة مستقلة، أو **مساحة فرعية**.
   - ضمن **معلومات المساحة**: **الاسم** (بكل لغة من لغاتك)، و**الوصف**، و**الأيقونة**.
   - ضمن **النطاق**: **معرف النطاق**، الذي يصبح الجزء الأول من عنوان المساحة. استخدم الأحرف الصغيرة والأرقام والشرطات السفلية فقط، مثل `hr`، ولكل مساحة معرّفها الخاص. أما **الرابط** (عنوانك الرئيسي) فيُملأ تلقائيًا ولا يمكن تغييره، ويتكوّن **الرابط الكامل** – مثل `hr.contoso.example.com` – من المعرّف والرابط.
   - **الصفحة الافتراضية** – اختياري: الصفحة التي يصل إليها الناس عند فتح المساحة.
3. اختر **حفظ**.

تظهر المساحة الجديدة على هيئة بطاقة في شاشة **المساحات**، ومعها عنوانها، ويُعِدّ أسس لك الصفحات الافتراضية للمساحة.

إضافة الأشخاص إلى مساحة

لا يرى الناس المساحة إلا إذا كانوا أعضاء فيها.

1. في **الإدارة › المساحات**، افتح قائمة بطاقة المساحة واختر **عرض المساحة**.
2. افتح تبويب **المستخدمين**، الذي يعرض قائمة أعضاء المساحة.
3. أضِف عضوًا: اختر **المستخدم**، وفعّل **مدير** إذا أردت تسجيله مسؤولًا عن المساحة.
4. اختر **حفظ**.

يستطيع العضو الجديد الانتقال إلى المساحة من **مساحاتي** في الشريط العلوي. ولإزالة شخص من مساحة، أزِل مُدخله من تبويب **المستخدمين**.

البحث عن عضو `Since 1.10`

يمكنك البحث باسم الشخص في تبويب **المستخدمين** الخاص بالمساحة، وترشيح النتائج حسب المستخدم. وبعد الترقية، يصبح البحث متاحًا في العضويات القائمة بمجرد أن تنتهي المنصة من إعادة فهرستها.

وضع مساحة في الصيانة أو إيقافها

لكل بطاقة مساحة في **الإدارة › المساحات** قائمة تضم مفتاحين مستقلين:

الإجراء	ما يحدث	متى تستخدمه
تعطيل واجهات المستخدم النهائي	لا يعود الناس قادرين على استخدام تطبيقات المساحة وصفحاتها وخدماتها، وتظل الإدارة تعمل، فتستطيع مواصلة تهيئة المساحة.	للصيانة: حين تغيّر تطبيقًا ولا تريد أن يستخدمه الناس قبل اكتماله.
إلغاء تفعيل المساحة	تتوقف المساحة كلها، ويتوقف عنوانها عن العمل لدى الجميع.	حين لا تعود المساحة مطلوبة، أو يلزم إغلاقها فورًا.

يتطلّب كل إجراء تأكيدًا، ويقابله إجراء لإعادة التشغيل: **تفعيل واجهات المستخدم النهائي** أو **تفعيل المساحة**، على الترتيب.

- لا يمكن تعطيل المساحة الافتراضية.
- يُسجَّل إيقاف واجهات المستخدم النهائي لمساحة ما أو إعادة تشغيلها في **الإدارة › المراقبة › سجل النظام**. راجع المراقبة: السجلات والتدقيق.

النطاقات

يتضمّن كل نطاق عنوانًا أو أكثر في **المضيف**، مع خيارات تسجيل الدخول الخاصة بهذه العناوين. ويحتوي التثبيت الجديد على نطاق واحد هو **Default Domain**. وتُحفظ مُدخلات النطاقات في كيان **النطاق**: افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح **النطاق**.

ويجب أن يشمل أحد النطاقات عنوان المساحة كي يتمكن الناس من تسجيل الدخول عبره. فإذا أضفت مساحة على عنوان جديد، فاطلب من المشغّل التأكد من إعداد العنوان للمنصة.

لا يمكنك أرشفة نطاق لا تزال معارض أو تقارير تستخدمه؛ إذ يعرض أسس الرسالة *You can't archive this domain because it is being used*. ويسرد تلك المعارض والتقارير. لذا وجّهها أولًا إلى نطاق آخر.

خيارات تسجيل الدخول لكل نطاق

يحدّد كل نطاق ما تعرضه صفحة تسجيل الدخول الخاصة به. ولتغيير ذلك، افتح مُدخل النطاق، واختر **تعديل**، واضبط هذه الحقول، ثم اختر **حفظ**:

الحقل	حين يكون مفعّلًا
السماح بتسجيل المستخدم	يستطيع الناس تسجيل الدخول باستخدام اسم مستخدم أو بريد إلكتروني، مع كلمة مرور.
دعم مفاتيح المرور	يستطيع الناس تسجيل الدخول بمفتاح مرور (بصمة الإصبع أو الوجه أو رمز PIN للجهاز)، وإضافة مفاتيح مرور إلى حساباتهم.
رسائل نصية للمصادقة الثنائية	بعد إدخال كلمة المرور، يجب على الناس إدخال رمز يُرسل إلى هواتفهم برسالة نصية.
البريد الإلكتروني للمصادقة الثنائية	بعد إدخال كلمة المرور، يجب على الناس إدخال رمز يُرسل إلى عناوين بريدهم الإلكتروني.
السماح بالتحقق بكلمة المرور	يستطيع من ليست لديهم وسيلة للتحقق بعامل ثانٍ تأكيد هويتهم بكلمة المرور قبل عرض قيمة محمية.

أما أزرار الدخول الموحّد، مثل **Sign in with Microsoft**، فيربطها المشغّل بالنطاق. ولمعرفة معنى كل خيار، وكيف تعمل عوامل التحقق الثانية معًا، وكيفية إعداد الدخول الموحّد، راجع طرق تسجيل الدخول والدخول الموحّد.

معلومات مفيدة

- **كل عنوان يتبع مساحة واحدة.** إذا لم تستخدم أي مساحة عنوانًا ما، فإنه يعرض خطأ «غير موجود» بدلًا من فتح مساحة. `Since 1.10`
- **التصاميم الخاصة تبقى في مساحتها.** الكيانات والمعارض التي تُشارَك بصورة خاصة مع مساحة واحدة لا تظهر في قوائم مساحة أخرى. `Since 1.10`
- **تسري تغييرات العضوية فورًا.** فمن يُضاف إلى مساحة يستطيع الانتقال إليها في الحال، ومن يُزال منها يفقد الوصول إليها في الحال.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
أُضيف شخص إلى مساحة لكنه لا يراها.	تحقّق من وجود مُدخله في تبويب **المستخدمين** الخاص بالمساحة، ومن أن المساحة وواجهات المستخدم النهائي فيها مفعّلة. واطلب منه إعادة تحميل الصفحة أو تسجيل الدخول مجددًا.
يعرض عنوان مساحة الخطأ «غير موجود».	ربما تكون المساحة معطّلة، أو لم يُعَدّ العنوان بعد. تحقّق من المساحة في **الإدارة › المساحات**، ثم راجع المشغّل.
لا يستطيع الناس استخدام تطبيقات مساحة ما، لكن الإدارة تعمل.	واجهات المستخدم النهائي فيها معطّلة. اختر **تفعيل واجهات المستخدم النهائي**.
لا يمكنك تعطيل مساحة.	لا يمكن تعطيل المساحة الافتراضية ولا المساحات التي أنشأتها المنصة لنفسها.
لا يمكنك أرشفة نطاق.	لا تزال معارض أو تقارير تستخدمه. انقلها إلى نطاق آخر أولًا.

> **للتعمّق أكثر**
>
> للمشغّلين ومطوّري التكامل: المساحات والنطاقات: مرجع تقني · عمليات بوابة الـ API

التحقق البشري (الحماية من الروبوتات)

`Since 1.8`

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتشرح كيف يتحقق أسس من أن مستخدم نماذجك العامة وصفحات تسجيل الدخول شخص حقيقي لا روبوت، وكيف تفعّل هذا التحقق على نموذج عام، وما العمل حين يُبلغك المستخدمون بأنهم لا يستطيعون اجتيازه.

كيف يعمل

يحمي أسس موضعين مختلفين، وتختلف طريقة التحقق في كلٍّ منهما:

	النماذج العامة	صفحات تسجيل الدخول
ما المحمي	النماذج وعمليات البحث التي يستخدمها الزوار **دون تسجيل الدخول**.	تسجيل الدخول، وخطوة العامل الثاني، وإعادة تعيين كلمة المرور المنسية.
من يفعّله	بُناة التطبيقات لديك، لكل نموذج على حدة، ويظل معطّلًا حتى يفعّلوه.	المشغّل، للمنصة بأكملها، وهو مفعّل افتراضيًا.
ما يراه الناس	مربع **لست روبوت**. يحدّدونه، وينتظرون لحظة حتى تظهر علامة الصح، ثم يرسلون النموذج.	لا شيء. يجري التحقق تلقائيًا عند الإرسال، وأقصى ما قد يلاحظونه توقّف قصير.
إذا تعطّلت خدمة التحقق	لا يستطيع الزوار إرسال النماذج المحمية، ويستمر كل ما عداها في العمل.	**لا يستطيع أحد تسجيل الدخول**، ولا إكمال الخطوة الثانية، ولا إعادة تعيين كلمة المرور.

لا يُطلب من الزائر حلّ أحجية صور أو كتابة نص مشوَّه؛ إذ يُجري متصفحه عملية حسابية صغيرة في الخلفية يسهل على متصفح حقيقي إجراؤها، لكنها تصبح مكلفة لروبوت يكرّرها آلاف المرات.

ولا يُطلب من المستخدمين الذين سجّلوا الدخول إجراء التحقق على النماذج أبدًا، فهو مخصّص للزوار وحدهم.

مثال. تنشر إدارة الموارد البشرية لديك نموذجًا عامًا للتقدّم إلى الوظائف. ومن دون حماية، قد ترسل الروبوتات آلاف الطلبات المزيّفة. أما عند تفعيل التحقق البشري، فيحدّد كل متقدّم **لست روبوت** قبل الإرسال، وبذلك يمنع التحقق الروبوتات من إرسال الطلبات.

تفعيله على نموذج عام

يجري ذلك في معرض النموذج، وعادةً على يد باني التطبيقات الذي نشره.

1. افتح المعرض للتحرير وانتقل إلى إعدادات **أذونات الوصول** الخاصة به.
2. تأكد من تفعيل **مجهول**؛ إذ لا ينطبق التحقق إلا على المعارض التي يستطيع الزوار فتحها دون تسجيل الدخول.
3. حدّد **التحقق البشري**.
4. احفظ المعرض وانشره.

إتاحة المعرض للعامة لا تفعّل التحقق تلقائيًا، فهو خيار منفصل. ولمعرفة كيفية إتاحة النموذج للعامة أصلًا، راجع معارض البيانات [بناء التطبيقات › معارض البيانات وأوجهها].

ما الذي يحميه

في المعرض المحمي، يجب على الزائر اجتياز التحقق كي:

- يرسل مُدخلًا جديدًا؛
- يغيّر مُدخلًا؛
- يُجري بحثًا في المعارض التي تطلب من الزوار البحث قبل رؤية أي نتائج.

أما مجرد فتح قائمة عامة فلا يتطلب تحققًا.

صفحات تسجيل الدخول محمية أيضًا `Since 1.8`

تتحقق صفحات تسجيل الدخول، بصورة مستقلة عن النماذج، من أن من يسجّل الدخول شخص حقيقي. ويسري ذلك على الجميع وفي كل نطاق، ولا تتوفر له إعدادات في **الإدارة**؛ فالمشغّل وحده يستطيع إيقافه، ويشمل الإيقاف المنصة بأكملها.

ولأن هذا التحقق غير مرئي، لا يلاحظه المستخدمون إلا حين يفشل. وعند فشله، يرون الرسالة نفسها التي تظهر عند إدخال كلمة مرور خاطئة، لذا قد ترجع شكوى المستخدم «لا أستطيع تسجيل الدخول» إلى أيٍّ من السببين.

> ⚠ **إذا لم يستطع أحد تسجيل الدخول**
>
> إذا تعذّر فجأةً على **الجميع** تسجيل الدخول أو إكمال الخطوة الثانية أو إعادة تعيين كلمة المرور، فاطلب من المشغّل أن يفحص خدمة التحقق البشري أولًا. فهذا التحقق لا يسمح بمرور أحد حين تكون الخدمة معطّلة، بل يمنع تسجيل الدخول إلى أن تعود الخدمة إلى العمل أو يوقف المشغّل التحقق.

وتجد شرحًا لهذه الخطوة من منظور المستخدم النهائي في تسجيل الدخول واختيار مساحة [استخدام أسس].

معلومات مفيدة

- **كل تحقق يُستخدم مرة واحدة.** فإذا ترك الزائر النموذج مفتوحًا لأكثر من خمس دقائق تقريبًا، طُلب منه التحقق مجددًا.
- **لا إعدادات تُضبط.** فالمشغّل هو من يحدّد مستوى صعوبة العملية الحسابية ومدة صلاحية التحقق للمنصة بأكملها.
- **المتصفحات القديمة جدًا أو المقيّدة بشدة** التي تحجب التحقق لا تستطيع إرسال النماذج المحمية.
- **يحتاج التحقق في صفحة تسجيل الدخول إلى عنوان آمن.** فلا يمكن تشغيل التحقق في صفحة تسجيل دخول تُقدَّم دون HTTPS، ولذلك يجب على المشغّل إيقافه هناك.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
يتلقى زائر عند الإرسال رسالة خطأ تفيد بأن التحقق البشري مطلوب.	لم يُجرِ التحقق، أو انتهت صلاحية التحقق الذي أجراه، أو سبق استخدامه. اطلب منه تحديد **لست روبوت** مجددًا ثم الإرسال.
يعرض مربع **لست روبوت** الرسالة *فشل التحقق، يرجى المحاولة مرة أخرى.*	اطلب منه المحاولة مجددًا. وإذا استمر الفشل لدى الجميع، فاطلب من المشغّل فحص خدمة التحقق البشري.
يبدو أن تفعيل التحقق لا أثر له.	يجب أن يكون المعرض متاحًا للزوار من نوع **مجهول**؛ فالمستخدمون الذين سجّلوا الدخول لا يرون التحقق أبدًا.
لا يستطيع أي زائر إرسال أي نموذج محمي.	الأرجح أن خدمة التحقق البشري معطّلة. راجع المشغّل.

ما تراه	ما الذي تتحقق منه
لا يستطيع أحد تسجيل الدخول إطلاقًا.	راجع إذا لم يستطع أحد تسجيل الدخول، واطلب من المشغّل فحص خدمة التحقق البشري.
يفشل تسجيل الدخول لأول شخص يحاول بعد فترة خمول، ثم يعمل.	كانت خدمة التحقق في طور بدء التشغيل بعد الخمول. وإذا تكرر ذلك كثيرًا، فاطلب من المشغّل مراجعة مهلتها.
يُبلغ مستخدمون سجّلوا الدخول عن «CAPTCHA».	ليس مصدره أسس: فالمستخدمون الذين سجّلوا الدخول لا يُطلب منهم التحقق على النماذج أبدًا.

للتعمّق أكثر

للمشغّلين: التحقق البشري: مرجع تقني · مخطط Helm – التحقق البشري على صفحات الهوية

المظهر: السمات والخطوط والأيقونات

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتوضّح لك كيف تضفي على أسس مظهر مؤسستك: بإضافة خطوطك وسماتك الخاصة، واختيار السمات المتاحة للمستخدمين، ونشر أيقوناتك الخاصة. أما اللغات والمناطق الزمنية وصيغ التاريخ فتجدها في إعدادات المنظمة.

كيف يعمل

- **الخط** هو الخط الطباعي الذي ترفعه، مثل الخط المعتمد في شركتك.
- **السمة** مظهر له اسم، يحدّد الألوان والخطوط المستخدمة وما إذا كان المظهر داكنًا.
- **مُدخل الإعدادات** يحدّد السمات التي يستطيع المستخدمون الاختيار من بينها، والسمة الافتراضية لهم، على مستوى منظمتك بأكملها، أو مساحة واحدة، أو مستخدم واحد. وتجد شرحًا لطريقة عمل مُدخلات الإعدادات في إعدادات المنظمة.

اتّبع هذا الترتيب: ارفع الخطوط، ثم أنشئ سمات تستخدمها، ثم أتِح السمات عبر مُدخل إعدادات.

مثال. تستخدم علامتك التجارية الخط *Contoso Sans*. ارفعه، وأنشئ سمة فاتحة باسم *Contoso Day* وسمة داكنة باسم *Contoso Night* تستخدم كلتاهما هذا الخط، ثم أتِح السمتين للجميع في مُدخل إعدادات منظمتك، واجعل *Contoso Day* السمة الافتراضية.

تجد الخطوط والسمات ضمن **الإدارة › الواجهات**. وتظهر **الواجهات** لمن لديه صلاحية **مطور** على الأقل على مستوى النظام، أما إضافة المُدخلات أو تعديلها فتتطلب مستوى **تعديل**.

إضافة خط

1. افتح **الإدارة › الواجهات › الخطوط**، ثم اختر **إضافة خط**.
2. املأ النموذج:
   - **اسم الخط** – الاسم الذي سيراه المستخدمون عند اختيار الخط.
   - **اللغة** – اللغات التي خُصّص لها الخط.
   - **WOFF** و**WOFF2** و**TTF** و**OTF** – ارفع الخط بكل صيغة من صيغ الملفات الأربع، فجميعها مطلوبة ليتمكن كل متصفح وجهاز من استخدامه.
3. اختر **حفظ**.

إضافة سمة

1. افتح **الإدارة › الواجهات › السمات**، ثم اختر **إضافة سمة**.
2. املأ النموذج:
   - **اسم السمة** – الاسم الذي سيراه المستخدمون.
   - **الوضع الليلي** – فعّله للسمة الداكنة.
   - **الخطوط المستخدمة** – الخطوط التي تستخدمها السمة.

- **التنسيق العام** – اختياري. ورقة أنماط تتضمن ألوان السمة وتنسيقها في تطبيق الويب.
- **التخصيص العام للموبايل** و**خط التطبيق** – الألوان والخط اللذان تستخدمهما السمة في تطبيق الهاتف المحمول.

3. اختر **حفظ**.

اختيار السمات التي يستطيع الناس استخدامها

لا تُتاح السمة لأحد ما لم تُدرَج في مُدخل إعدادات.

1. افتح **الإدارة › الواجهات › الإعدادات**، ثم افتح المُدخل الخاص بمنظمتك، أو بمساحة، أو بشخص (أو أضِف مُدخلًا). قد لا تعرض القائمة إلا مُدخل **المنظمة**؛ راجع المشكلة المعروفة في ضبط الإعدادات الافتراضية لمنظمتك.
2. في **السمات المتاحة**، حدّد السمات التي تريد إتاحتها. وفي **السمة الافتراضية**، حدّد السمة التي يستخدمها المستخدمون إلى أن يختاروا غيرها.
3. اختر **حفظ**.

وللاطلاع على القائمة الكاملة لحقول مُدخل الإعدادات، راجع اضبط الإعدادات الافتراضية لمنظمتك.

الزوار الذين لم يسجّلوا الدخول

تستخدم الصفحات والنماذج العامة مُدخل الإعدادات الخاص بالمساحة التي تنتمي إليها فقط؛ فلا ينطبق مُدخل منظمتك ولا المُدخلات الشخصية على الزوار. وإذا لم يكن للمساحة مُدخل إعدادات، يظهر للزوار المظهر الافتراضي المدمج. ولكي تظهر الصفحات العامة بمظهرك، أضِف مُدخل إعدادات لتلك المساحة.

نشر أيقوناتك الخاصة `Since 1.8`

يمكنك إضافة أيقوناتك الخاصة، مثل شعارات الإدارات، واستخدامها في كل موضع يتيح فيه أسس للمستخدمين اختيار أيقونة.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **الأيقونات**.
2. أضِف مُدخلًا: أدخل **الاسم**، والصق رماز **SVG** الخاص بالأيقونة، وأضِف **الوسوم** لتسهيل العثور عليها، وفعّل **اتجاهي** إذا كان ينبغي عكس الأيقونة في اللغات التي تُكتب من اليمين إلى اليسار، كما في أيقونة السهم مثلًا.
3. اختر **حفظ**.

وتصل مجموعة الأيقونات الجديدة تلقائيًا إلى من يستخدمون أسس في تلك اللحظة، دون حاجة إلى تحديث أي شيء.

هياكل التطبيقات `Since 1.10`

تتضمن السمة حقلًا اختياريًا هو **هيكلية التطبيق**، وقد ترى كيانًا باسم **هيكلية التطبيق**، وكلاهما محجوز لأداة مرئية لبناء الهياكل ليست جزءًا من الإصدار 1.10. وعند إرفاق هيكل بسمة، يُحفظ هذا الاختيار، لكنه لا يغيّر شيئًا مما يراه المستخدمون.

مصدر اسمك وشعارك `Since 1.10`

لا يُضبط اسم المنتج ولا الشعارات ولا أيقونة الموقع ولا السمة الأساسية ولا شاشة التحميل في تطبيق الويب من هذه الصفحة؛ إذ تُستمد هذه العناصر من إعدادات النشر لديك، وكذلك من العلامة التجارية لمؤسستك في النشر المشترك. أما

سماتك فتغيّر مظهر التطبيق المحيط بهذه العناصر. ولتغيير الاسم أو الشعار، اطلب ذلك من المشغّل. راجع اسم منظمتك وشعارها وصفحة تسجيل الدخول.

ويصل أي تغيير يُجريه المشغّل على علامتك التجارية إلى متصفحات المستخدمين خلال ساعة، بما في ذلك النسخ المثبّتة من تطبيق الويب.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
سمة جديدة غير متاحة لأحد.	أضِفها إلى **السمات المتاحة** (أو اجعلها **السمة الافتراضية**) في مُدخل الإعدادات الذي ينطبق على هؤلاء المستخدمين.
شخص واحد يرى مظهرًا مختلفًا عن الجميع.	لديه مُدخل إعدادات شخصي، أو لمساحته مُدخل إعدادات. وللمُدخلات الشخصية ومُدخلات المساحات أولوية على مُدخل المنظمة.
لا يظهر أحد الخطوط.	تحقّق من أن السمة تستخدمه ضمن **الخطوط المستخدمة**، ومن أن السمة متاحة في مُدخل الإعدادات الصحيح.
لا يوجد مُدخل إعدادات لأحد، ومع ذلك يرى الناس سمة.	هذه هي السمة الافتراضية المدمجة، وتُستخدم حين لا ينطبق أي مُدخل إعدادات.

للتعمّق أكثر

للمشغّلين ومطوّري التكامل: إعدادات القاطن والمظهر: مرجع تقني

المراقبة: السجلات والتدقيق

هذه الصفحة موجّهة إلى مسؤولي القاطن، وتبيّن لك كيف تستخدم شاشات **المراقبة** للإجابة عن ثلاثة أسئلة يومية: «هل أُرسلت هذه الرسالة؟» و«هل شُغّلت هذه الأتمتة، وماذا فعلت؟» و«من غيّر هذا؟» كما تشرح من يستطيع الاطّلاع على هذه الشاشات، ومدة الاحتفاظ بالسجلات.

كيف تعمل

يحتفظ أسس بنوعين من السجلات التاريخية:

- **السجلات** تدوّن ما *فعلته* المنصة: كل رسالة بريد إلكتروني ورسالة نصية ورسالة واتساب حاولت إرسالها، وكل تشغيل لعملية أتمتة، وكل مرة أُوقفت فيها واجهات المستخدم النهائي لمساحة ما أو أُعيد تشغيلها.
- **سجل التدقيق** يدوّن من *غيّر* ماذا: المُدخلات، وتصاميم الكيانات، والمعارض، والأذونات، والمساحات، وحسابات المستخدمين، وغير ذلك.

ويمكنك الاطّلاع على كليهما ضمن **الإدارة › المراقبة**:

الشاشة	تجيب عن	من يستطيع فتحها
السجلات	هل أُرسلت الرسالة، وهل وصلت؟ التنبيهات **البريد الإلكتروني** و**الرسائل النصية** و**واتساب**.	مسؤولو النظام
سجل النظام	من أوقف واجهات المستخدم النهائي لمساحة ما أو أعاد تشغيلها، ومتى؟	مسؤولو النظام
سجل التدقيق	من غيّر ماذا، ومتى؟	مسؤولو النظام
سجل التفاعلات `Since 1.10`	هل شُغّلت عملية أتمتة، وماذا فعل كل إجراء من إجراءاتها؟	مسؤولو النظام

مثال. تقول موظفة إنها لم تتلقَّ رسالة البريد الإلكتروني التي تؤكد اعتماد إجازتها مطلقًا. تفتح **سجل التفاعلات** فتجد أن الأتمتة *اعتماد الإجازة* قد شُغّلت لطلبها، وأن إجراء **إرسال البريد الإلكتروني** فيها نجح. ثم تفتح **السجلات › البريد الإلكتروني**، وتجد الرسالة التي تحمل **رقم التفاعل** نفسه، فترى أن **الحالة** هي **نجاح**؛ أي إن الرسالة غادرت المنصة، فتكون الخطوة التالية أن تبحث الموظفة في مجلد الرسائل غير المرغوب فيها لديها.

التحقق مما إذا أُرسلت رسالة

1. افتح **الإدارة › المراقبة › السجلات**.
2. اختر تبويب **البريد الإلكتروني** أو **الرسائل النصية** أو **واتساب**.
3. رتّب حسب **تاريخ الإرسال** لترى أحدث الرسائل أولًا، وتنقّل بين الصفحات حتى تصل إلى الرسالة التي تبحث عنها.
4. حدّد صفًا لعرض تفاصيله.

في تبويب البريد الإلكتروني، تعرض القائمة **رقم التفاعل** و**المرسل إلى** و**المرسل** و**نسخة إلى** و**نسخة مخفية** و**الموضوع** و**تاريخ التوليد** و**تاريخ الإرسال** و**الحالة**، كما تعرض التفاصيل **رمز الاستجابة** الصادر عن خادم البريد. وتكون **الحالة نجاح** حين يقبل خادم البريد الرسالة، و**فشل** حين لا يقبلها.

ويربط **رقم التفاعل** الرسالةَ بتشغيل الأتمتة الذي أرسلها. فإذا كنت تعرف الأتمتة التي كان ينبغي أن ترسل الرسالة، فابدأ من سجل التفاعلات وطابق الرقم؛ فهذا غالبًا أسرع من التنقّل بين صفحات سجل الرسائل.

نسخ رسائل البريد لا تحتوي على أسرار

لا تحتوي نسخة الرسالة المحفوظة في السجل أبدًا على رابط إعادة تعيين كلمة المرور ولا على رمز API، إذ يُستبدل بهما `[redacted]`. أما سائر محتوى الرسالة فيُحفظ، لذا لا تُدرج الأسرار في القوالب. راجع الإشعارات وقوالب البريد الإلكتروني.

رسائل واتساب `Since 1.10`

يضم تبويب **واتساب** صفًا لكل رسالة، مرتّبًا من الأحدث إلى الأقدم، ويعرض تشغيل التفاعل، والمستلم، والقالب ولغته، ووقت الإرسال، والحالة.

الحالة	المعنى
مقبولة، **مرسلة**، **تم التسليم**، **مقروءة**	قبلت Meta الرسالة، ثم أبلغت عن المرحلة التي وصلت إليها، وتظهر هذه الحالات على أنها ناجحة.
فشل	لم تُرسل الرسالة، أو أبلغت Meta عن فشل. افتح الصف لترى الخطأ الذي أبلغت عنه Meta.
لم تُرسل (الإرسال معطل)	الإرسال الفعلي عبر واتساب غير نشط في بيئة النشر لديكم. اطلب من المشغّل تفعيله.

افتح صفًا لترى **السجل التاريخي للحالات** الخاص به. وتبقى القيم التي عُبّئ بها القالب مخفية إلى أن تختار **عرض متغيرات القالب**. ولا تُخزَّن رموز تسجيل الدخول أبدًا.

ولا تظهر حالتا التسليم والقراءة إلا إذا كان تطبيق واتساب الخاص بكم في Meta يرسل تقارير التسليم إلى أسس. راجع ربط واتساب.

التحقق مما إذا جرى تشغيل أتمتة `Since 1.10`

تسرد شاشة **الإدارة › المراقبة › سجل التفاعلات** كل تشغيل لعملية أتمتة (تفاعل) في المساحة الحالية، مرتّبًا من الأحدث إلى الأقدم. استخدم السجل للإجابة عن السؤال: «هل شُغّل التفاعل الخاص بي، وماذا فعل؟»

1. افتح **الإدارة › المراقبة › سجل التفاعلات**.
2. ضيّق نطاق القائمة باستخدام المرشّحات السريعة **التفاعل** و**الحدث** و**الإجراء** و**الحالة** و**الفترة الزمنية** (**آخر يوم**، **آخر أسبوع**، **آخر شهر**، **آخر سنة**)، أو اكتب في مربع البحث. ويطابق البحث اسم التفاعل، أو كيانه أو وحدته، أو الشخص الذي أطلقه، أو معرّف تشغيل أو مُدخل بمطابقة تامة.
3. حدّد تشغيلًا لفتح تفاصيله: جميع حقول التشغيل، ونتيجة كل إجراء، و**عرض JSON** للسجل الكامل. واستخدم زرَّي السابق والتالي للتنقّل في القائمة المرشَّحة.

الأعمدة هي **اسم التفاعل** و**الحالة** و**الوقت** و**المدخل** و**الفاعل** و**نوع الحدث** و**نوع الإجراء** و**الكيان** و**الوحدة**. ويمكنك إعادة ترتيبها خلال جلستك، ويبقى عمود **التفاصيل** في النهاية.

- **الحالة.** يُعدّ التشغيل فاشلًا إذا فشل أي من إجراءاته، وناجحًا إذا نُفِّذ إجراء واحد على الأقل دون أن يفشل أي إجراء. وتعني **بدون إجراءات** أن التشغيل لم ينفّذ أي إجراء.
- **لا تُسرد إلا التشغيلات التي نُقّذت.** لا يظهر صف للتفاعل إذا لم يطابق مرشّحُه الحدثَ. فإذا كنت تتوقع تشغيلًا ولم تجده، فتحقّق من مرشّح التفاعل.
- **المدخل.** تعني *مدخل محذوف أو غير معروف* أن المُدخل لم يعد موجودًا، وتعني *غير محدد* أنه موجود لكن لا عنوان له.
- **تبقى المرشّحات في العنوان**، لذا يعرض زر الرجوع في المتصفح والرابط المشترك القائمة نفسها.

- **من مصمّم الكيانات.** في تبويب **التفاعلات** الخاص بالكيان، يستطيع مسؤول النظام تحديد عدد التشغيلات الفاشلة أو الناجحة لتفاعل ما للاطّلاع على التشغيلات التي يشملها هذا العدد، مع روابط إلى كل تشغيل وإلى هذه الشاشة بعد تطبيق المرشّحات عليها مسبقًا.

الأسرار مخفية هنا أيضًا. تُخزَّن القيم التي وضع عليها باني التطبيقات علامة **محجوب في السجل التاريخي**، والقيم الواردة من الحقول الحسّاسة، والأسرار المعروفة مثل كلمات المرور والرموز المميزة ومفاتيح API، بالصيغة `****`، فلا يراها حتى مسؤول النظام. `Since 1.6`

مراجعة من غيّر ماذا

1. افتح **الإدارة › المراقبة › سجل التدقيق**.
2. استخدم البحث والمرشّحات لتضييق نطاق القائمة – حسب **اسم الحدث** أو **المستخدم** أو **تاريخ السجل** مثلًا.
3. افتح سجلًّا لترى **التفاصيل** الخاصة به: ما الذي تغيّر، وإذا كان التغيير في مُدخل، فأي الحقول تغيّرت وما قيمها القديمة والجديدة.

تظهر في **اسم الحدث** أسماء واضحة مثل *تم تسجيل دخول المستخدم*، و*إعادة تعيين كلمة المرور بواسطة المسؤول*، و*تم قفل حساب المستخدم*، و*تم تحديث سجل البيانات*، و*تم تحديث كيان البيانات*، و*تم تغيير حقوق الوصول*، و*تم إلغاء تنشيط مساحة العمل*، و*تم تحديث تفاعل*، و*تم استيراد الحزمة*، و*تم الحذف الدائم لسجل البيانات*.

ما الذي يُسجَّل

- **الأشخاص:** عمليات تسجيل الدخول، وتغيير كلمات المرور وإعادة تعيينها، وتفعيل الحسابات أو تعطيلها أو قفلها.
- **المُدخلات:** الإنشاء والتحديث والأرشفة والاستعادة والحذف (بما في ذلك المسودات والإجراءات الجماعية).
- **التصميم:** إنشاء الكيانات وحقولها، والمعارض، والصفحات، والوحدات، والقوائم، والعلاقات، والاستعلامات، والتفاعلات، أو تغييرها أو حذفها.
- **الوصول:** كل تغيير في الأذونات.
- **المساحات:** الإنشاء والتحديث والتفعيل والتعطيل، وإيقاف واجهات المستخدم النهائي أو إعادة تشغيلها.
- **الرموز والحزم:** توليد رموز التطبيقات، وتصدير الحزم أو استيرادها.
- **البيانات الحساسة:** راجع ما يلي.

ما الذي لا يُسجَّل

- التغييرات التي تُجريها المنصة على نفسها، مثل الترقيات وترحيل البيانات.
- التغييرات على الإشعارات والطلبات وسجل التدقيق نفسه.
- قيم الحقول الحسّاسة: إذ تُخزَّن بالصيغة `***` للجميع وبصورة دائمة، ولا يمكنك استرجاعها من سجل التدقيق.

في حالات نادرة، مثل حدوث انقطاع قصير، قد يُفقد سجل تدقيق بعينه، لكن تعذّر كتابة سجل التدقيق لا يمنع التغيير نفسه ولا يُلغيه أبدًا.

كشف البيانات الحساسة `Since 1.10`

تُبيّن لك أربعة أحداث من اطّلع على القيم المحمية:

الحدث	يُسجَّل حين
تفعيل كشف البيانات الحساسة / إلغاء تفعيل كشف البيانات الحساسة	يبدأ شخص جلسة كشف أو يُنهيها.
كشف البيانات الحساسة	تُعرض قيمة حسّاسة فعلًا على شخص ما خلال جلسة كشف، بما في ذلك داخل تقرير.
فك تشفير	يكشف شخص قيمة حقل **مشفّر**.

ولا تُكتب القيم نفسها في سجل التدقيق أبدًا. أما عمليات التصدير ورسائل التقارير المجدولة فتتضمن القيم الحقيقية بحكم تصميمها، ولا تُسجَّل على أنها عمليات كشف. وتُحدّد الأذونات الحساسة من يستطيع تنفيذ العمليات التي تُسجَّل بهذه الأحداث.

التحقق من الهوية قبل الكشف

قبل أن يكشف شخص قيمة مشفّرة أو يشغّل إجراءً في سير العمل يطلب منه تأكيد هويته، يطلب أسس التحقّق من الهوية مجددًا. وتُسجَّل كل محاولة، ناجحة كانت أم لا، في سجل أمان تسجيل الدخول الخاص بالمنصة، لا في شاشة **سجل التدقيق**، ولذلك يترك إدخال رمز خاطئ أثرًا حتى لو لم تُكشف أي قيمة. وإذا احتجت إلى هذه السجلات، فاطلبها من المشغّل.

الكيانات المحذوفة نهائيًا `Since 1.10`

عندما يحذف مسؤول النظام كيانًا حذفًا نهائيًا، يسجّل سجل التدقيق الحدث *تم الحذف الدائم للكيان* مع الكيان ووحدته والشخص الذي حذفه، ويمكنك تحديد هذا الحدث في مرشّح **اسم الحدث**.

رموز التطبيقات

عندما يطلب مسؤول إعادة توليد رمز API الخاص بمستخدم تطبيق، يُسجَّل هذا الطلب، أما الرمز نفسه فلا يُكتب في سجل التدقيق أبدًا. `Since 1.8`

تدوير رمز الوظيفة `Since dev`

في خط التطوير، لكل وظيفة مستخدم تطبيق خاص بها. وعندما تعيد توليد رمز ذلك المستخدم، يُرسل الرمز الجديد مباشرةً إلى الوظيفة، ويعرض سجل التدقيق طلبك إلى جانب سجل *Function App Token Regenerated*.

التحقق من تغييرات صيانة المساحات (سجل النظام)

تعرض شاشة **الإدارة › المراقبة › سجل النظام** كل مرة أُوقفت فيها واجهات المستخدم النهائي لمساحة ما أو أُعيد تشغيلها، مع **المستخدم** و**التاريخ** و**المساحة** و**الحالة** (**مُفعّل** أو **مُعطّل**). راجع المساحات والنطاقات.

من يستطيع رؤية هذه الشاشات

تظهر **المراقبة** لمن لديه صلاحية **إدارة** على مستوى النظام. ولقراءة سجلات الرسائل يحتاج المستخدم أيضًا إلى صلاحية **تعديل** أو **إدارة** على مستوى النظام كله، أما **سجل التفاعلات** فمتاح لمسؤولي النظام وحدهم؛ لأن تفاصيل التشغيل تتضمن ما قرأه كل إجراء وما كتبه. ويتبع ما يراه المستخدمون في **سجل التدقيق** كذلك أذونات وصولهم إلى سجلات التدقيق. راجع الأذونات والوصول.

مدة الاحتفاظ بالسجلات

تُحفظ سجلات أمان تسجيل الدخول والعامل الثاني 180 يومًا و90 يومًا على التوالي.

استكشاف الأخطاء وإصلاحها

السؤال	أين تبحث
«لم تصلني رسالة البريد الإلكتروني قط.»	**السجلات › البريد الإلكتروني**. تعني **نجاح** أن الرسالة غادرت المنصة؛ فتحقق من مجلد الرسائل غير المرغوب فيها. أما إذا كانت الحالة **فشل**، فافتح الصف للاطلاع على رمز الاستجابة وأرسله إلى المشغّل. وإذا لم تجد صفًا أصلًا، فلم تُرسل الأتمتة الرسالة؛ تحقق من **سجل التفاعلات**.
«لا تصل الرسائل النصية إلى أحد.»	**السجلات › الرسائل النصية**. إذا كان إرسال الرسائل يفشل أو لم تجد أي رسائل، فاسأل المشغّل عمّا إذا كان مزوّد الرسائل النصية (SMS) متصلًا.
يعرض واتساب **لم تُرسل (الإرسال معطل)**.	الإرسال الفعلي غير نشط في بيئة النشر لديكم. راجع المشغّل.
«هل جرى تشغيل الأتمتة الخاصة بي؟»	افتح **سجل التفاعلات** ورشّحه حسب التفاعل. وإذا لم تجد صفًا، فهذا يعني أن شروط مرشّح التفاعل لم تتحقق.
«من غيّر هذا المُدخل / هذا الإذن / هذا المعرض؟»	افتح **سجل التدقيق** ورشّحه حسب **اسم الحدث** و**تاريخ السجل**.
لا ترى **المراقبة** إطلاقًا.	تحتاج إلى صلاحية **إدارة** على مستوى النظام، ويجب أن تشمل رخصتك الإدارة. راجع رخصتك.

ⓘ للتعمّق أكثر

للمشغّلين ومطوّري التكامل: السجلات والتدقيق والاحتفاظ: مرجع تقني · قابلية المراقبة

الإشعارات وقوالب البريد الإلكتروني

هذه الصفحة موجّهة إلى مسؤولي القاطن. وتشرح كيف يتواصل أسس مع المستخدمين – داخل التطبيق، وبالبريد الإلكتروني، وبالرسائل النصية، وعبر واتساب – وما تديره بنفسك (القوالب المشتركة واتصال واتساب الخاص بمؤسستك)، وما يديره بُناة التطبيقات والمشغّل، وما تتحقق منه حين يقول أحدهم إن رسالة لم تصله قط.

كيف تعمل

تُرسل معظم الرسائل عبر **عمليات الأتمتة** (التفاعلات) التي يضيفها بُناة التطبيقات إلى تطبيقاتهم: «عند اعتماد طلب إجازة، أرسل بريدًا إلكترونيًا إلى الموظف». وتحدّد الأتمتة **متى** تُرسل الرسالة و**إلى من**، ويمكنها إنشاء نص الرسالة مباشرةً أو استخدام أحد **القوالب** المشتركة لديك.

القناة	ما يتلقاه المستخدمون	من يُعدّها
داخل التطبيق	إشعار تحت أيقونة الجرس في تطبيق الويب، وإشعار فوري على الهاتف لمن يستخدم تطبيق الهاتف المحمول.	بُناة التطبيقات، في عمليات الأتمتة.
البريد الإلكتروني	رسالة بريد إلكتروني.	بُناة التطبيقات، في عمليات الأتمتة. ويمكنك توفير قوالب مشتركة، بينما يربط المشغّل خادم البريد.
الرسائل النصية (SMS)	رسالة نصية.	بُناة التطبيقات، في عمليات الأتمتة، ويربط المشغّل مزوّد الرسائل النصية.
واتساب `Since 1.10`	رسالة واتساب تستند إلى قالب اعتمدته Meta.	تربط أنت رقم واتساب الخاص بمؤسستك، ويرسل بُناة التطبيقات الرسائل عبر عمليات الأتمتة، ويفعّل المشغّل الإرسال الفعلي.

وترسل المنصة أيضًا بعض الرسائل بنفسها، من دون أي أتمتة:

- رسالة البريد التي تتيح للمستخدم الجديد تعيين كلمة مروره، ورسالة إعادة تعيين كلمة المرور؛
- رسالة البريد التي تتضمن رمز API المولَّد حديثًا لمستخدم تطبيق؛
- إشعار حين يصبح ملف صدّره أحد المستخدمين في الخلفية جاهزًا للتنزيل؛
- رموز تسجيل الدخول، برسالة نصية أو بريد إلكتروني أو واتساب، حين يكون تسجيل الدخول بعامل ثانٍ مفعّلًا؛
- تحذيرات إلى مسؤولي النظام حين تقترب مؤسستك من حد المُدخلات. راجع حدود الخطة.

مثال. تريد إدارة الموارد البشرية أن يتلقى الموظفون رسالة بريد إلكتروني تحمل هوية الإدارة عند اعتماد إجازاتهم؛ فتنشئ قالب بريد إلكتروني باسم **اعتماد الإجازة** يتضمن ترويسة الموارد البشرية وتذييلتها، ثم يضيف باني التطبيقات إلى خدمة طلبات الإجازة أتمتةً ترسل هذا القالب إلى مقدّم الطلب عند اعتماد طلبه.

إدارة القوالب المشتركة

يُكتب القالب المشترك مرة واحدة وتستخدمه عمليات أتمتة متعددة، لذا ينعكس تغييره على كل رسالة تستخدمه.

نوع القالب	الغرض منه
بريد إلكتروني	رسالة بريد إلكتروني كاملة: الموضوع والمحتوى، مع ترويسة وتذييلة ومرفقات اختيارية.
أجزاء البريد الإلكتروني	ترويسة أو تذييلة قابلة لإعادة الاستخدام، مثل شعارك وعنوانك، تُدرج في قوالب البريد الإلكتروني.
إشعار	إشعار داخل التطبيق: عنوان ومحتوى.

إنشاء قالب بريد إلكتروني

1. افتح **الإدارة › الواجهات › القوالب**. (يمكنك أيضًا فتح **الإدارة › التطبيقات › الكيانات**، ثم فتح كيان **القوالب**.)
2. أضِف مُدخلًا واملأ ما يلي:
   - **اسم القالب** و**وصف القالب** – ليسهل على بُناة التطبيقات العثور على القالب المناسب.
   - **نوع القالب** – **بريد إلكتروني**.
   - ضمن **تفاصيل القالب**: **الموضوع** و**المحتوى**، واختياريًا **ترويسة القالب** و**تذييلة القالب** (اختر قوالب من نوع **أجزاء البريد الإلكتروني**).
   - **المرفقات** – ملفات اختيارية تُرسل مع كل رسالة بريد تستخدم القالب.
3. اختر **حفظ**.

أنشئ الترويسة والتذييلة أولًا بوصفهما قالبين من نوع **أجزاء البريد الإلكتروني**، لتتمكن من اختيارهما هنا. ويؤدي تغيير ترويسة أو تذييلة مشتركة إلى تحديث كل رسالة بريد تتضمنها.

العناصر النائبة

اكتب `{{ name }}` في الموضع الذي تريد إدراج قيمة فيه، مثل `Dear {{ employee_name }}, your leave from {{ start_date }} was approved.` ويمكن أن تتضمن الأسماء أحرفًا وأرقامًا وشرطات سفلية، ويحدّد باني التطبيقات الذي يستخدم القالب القيمة التي تحلّ محل كل عنصر نائب.

تغيير قالب قيد الاستخدام

يُفتح القالب للقراءة فقط. ولتغييره، اختر **تعديل قالب**، وأجرِ التغيير، ثم اختر **حفظ**.

عندما تحفظ قالبًا تستخدمه عمليات أتمتة بالفعل، يطلب منك أسس التأكيد: *هذا القالب مستخدم مسبقاً ضمن أحد التفاعلات. هل تريد حفظ جميع التغييرات ؟* ويسري التغيير على كل رسالة تُرسل بعد ذلك.

رسائل كلمات المرور

يمكن لرسائل البريد التي تتيح للمستخدمين تعيين كلمة المرور أو إعادة تعيينها استخدام قوالبك الخاصة: أنشئها بوصفها قوالب من نوع **بريد إلكتروني**، ثم اطلب من المشغّل استخدامها في صفحات تسجيل الدخول الخاصة بمؤسستك.

> ⚠ **أبقِ الأسرار خارج القوالب**
>
> تُحفظ نسخ من رسائل البريد المرسلة في سجل البريد الإلكتروني، الذي يستطيع مسؤولون آخرون قراءته، ويزيل أسس من تلك النسخ روابط إعادة تعيين كلمة المرور ورموز API فقط؛ لذا لا تضع أبدًا كلمات مرور أو رموزًا أو أي أسرار أخرى في قالب.

من يتلقى الرسالة

يحدّد بُناة التطبيقات المستلمين في كل أتمتة. ويمكنهم الإرسال إلى أشخاص محددين، أو إلى مجموعات، أو إلى قوائم أشخاص، أو إلى وحدات تنظيمية، أو إلى عناوين تُكتب يدويًا، أو إلى من يشير إليه المُدخل – مثل مقدّم الطلب، أو مالك الخطوة الحالية، أو مدير ذلك الشخص.

- لا يتلقى الأشخاص الذين عُطّلت حساباتهم رسائل البريد الإلكتروني.

- من كان سيتلقى رسالة البريد نفسها مرتين – بصفته شخصًا وبصفته عضوًا في مجموعة مثلًا – يتلقاها مرة واحدة.
- إذا تعذّر العثور على أحد المستلمين، تصل الرسالة إلى بقية المستلمين.

حين يكون أحدهم غائبًا: نسخ للمفوَّض له `Since 1.10`

إذا كان لدى شخص تفويض ساري المفعول مع تفعيل **حول الإشعارات** أو **حول البريد الالكتروني**، يتلقى المفوَّض له نسخة:

- **داخل التطبيق**، يتلقى المفوَّض له إشعارًا مستقلًا غير مقروء، مع علامة توضّح أنه محوَّل من الشخص الذي ينوب عنه.
- **بالبريد الإلكتروني**، يُضاف المفوَّض له إلى مستلمي النسخة، ويستمر المستلم الأصلي في تلقي الرسالة.

ولا يتلقى المفوَّض له نسخة ثانية إذا كان ضمن المستلمين أصلًا، ولا تُحوَّل النسخة مرة أخرى أبدًا. راجع التفويض – تحويل الإشعارات ورسائل البريد.

الإشعارات داخل التطبيق والإشعارات الفورية

تظهر الإشعارات داخل التطبيق تحت أيقونة الجرس في تطبيق الويب. ويتلقاها أيضًا على هاتفه، في صورة إشعارات فورية، كل من يستخدم تطبيق الهاتف المحمول ويسمح بالإشعارات. ولا يلزمك إجراء إعدادات لكل شخص على حدة، إذ يسجّل التطبيق كل هاتف عند تسجيل صاحبه الدخول.

النقر على إشعار `Since 1.10`

يؤدي النقر على الإشعار إلى وضع علامة عليه بأنه مقروء وفتح المحتوى المرتبط به: فالإشعارات التي ترسلها عمليات الأتمتة تفتح المُدخل الذي تشير إليه عبر المعرض الذي اختاره باني التطبيقات، أما بعض الإشعارات الصادرة عن المنصة نفسها، كإشعارات مراجعة الحزم من سوق التطبيقات، فتفتح صفحة محددة مباشرةً.

الهواتف التي تتوقف عن تلقي الإشعارات الفورية `Since 1.10`

يتلقى كل هاتف إشعارًا فوريًا واحدًا لكل رسالة، ويحذف أسس من قائمته الهواتف التي لم يتصل تطبيق الهاتف المحمول منها بالمنصة منذ 90 يومًا، والهواتف التي تُبلغ خدمة الإشعارات الفورية بأنها لم تعد صالحة. ويستأنف الشخص الذي حُذف هاتفه من القائمة تلقي الإشعارات الفورية بعد تسجيل الدخول مجددًا إلى تطبيق الهاتف المحمول والسماح بالإشعارات.

البريد الإلكتروني

تُرسل رسائل البريد من عنوان المرسِل الخاص بمؤسستك، ما لم تحدّد الأتمتة مرسِلًا آخر. ويضبط المشغّل عنوان المرسِل ويربط خادم البريد. وعندما تضيف الأتمتة رابطًا إلى المُدخل، يُختصر الرابط في الرسالة.

روابط إعادة تعيين كلمة المرور ورموز API لا تصل أبدًا إلى سجل البريد الإلكتروني. فالرسالة تصل إلى الشخص كاملة، لكن هذين السرّين يُستبدلان بـ `[redacted]` في النسخة المحفوظة في سجل البريد الإلكتروني. `Since 1.4`

الرسائل النصية (SMS)

تُرسل الرسائل النصية عبر مزوّد رسائل نصية يربطه المشغّل. ولا تُرسل أي رسائل نصية حتى يُربط مزوّد. وإذا لم تصل أي رسائل نصية إطلاقًا، فاسأل المشغّل عمّا إذا كان قد أعدّ مزوّدًا.

واتساب `Since 1.10`

تستخدم رسائل واتساب دائمًا قالب رسالة اعتمدته Meta لحساب WhatsApp Business الخاص بكم، ولا يرسل أسس نصًا حرًا عبر واتساب أبدًا.

- **لإعداده**، اربط رقم واتساب الخاص بكم في إعدادات النظام. راجع ربط واتساب.
- **يرسل بُناة التطبيقات الرسائل** باستخدام الإجراء **إرسال رسالة واتساب** ضمن إحدى عمليات الأتمتة، ويختارون أحد قوالبكم المعتمدة. وإذا لم يكن رقمكم مربوطًا، يعرض الإجراء التنبيه: *لم يتم إعداد واتساب لهذه المساحة. أكمل قسم واتساب في إعدادات النظام أولًا.* راجع التفاعلات والأتمتة [بناء التطبيقات].
- **رموز تسجيل الدخول** يمكن إرسالها أيضًا عبر واتساب. راجع رموز واتساب.

لكل رسالة واتساب صف في سجل رسائل واتساب:

الحالة	معناها	ما الذي تفعله
مقبولة، **مرسلة**، **تم التسليم**، **مقروءة**	قبلت Meta الرسالة، ثم تُبلغ عن المرحلة التي وصلت إليها.	لا شيء.
لم تُرسل (الإرسال معطل)	الإرسال الفعلي عبر واتساب غير نشط في بيئة النشر لديكم، ولم يصل شيء إلى Meta.	اطلب من المشغّل تفعيل الإرسال الفعلي، إذ يظل متوقفًا حتى يفعّله.
فشل	لم تُرسل الرسالة، أو رفضتها Meta. افتح الصف لمعرفة السبب.	الأسباب الشائعة: رقمكم غير مربوط بهذه المساحة، أو رقم المستلم ليس بالصيغة الدولية (`+` ورمز البلد)، أو رفضت Meta الرسالة.

ولا تُعاد تلقائيًا محاولة إرسال رسالة لم تقبلها Meta إلا عند التأكد من أنها لم تُرسل، كي لا يتلقى أحد الرسالة نفسها مرتين. ولا تُخزَّن رموز تسجيل الدخول في السجل أبدًا.

استكشاف الأخطاء وإصلاحها

يقول أحدهم…	ما الذي تتحقق منه
«لم تصلني رسالة البريد قط.»	افتح **الإدارة › المراقبة › السجلات**، ثم انتقل إلى تبويب **البريد الإلكتروني**، وابحث عن الرسالة وتحقق من **الحالة**. وإذا لم تجد صفًا لها، فهذا يعني أن الأتمتة لم ترسلها: تحقق من الأتمتة في **الإدارة › المراقبة › سجل التفاعلات**. راجع المراقبة: السجلات والتدقيق.
«لا تصل الرسائل النصية إلى أحد.»	اسأل المشغّل عمّا إذا كان مزوّد الرسائل النصية مربوطًا.
«يقول واتساب: *لم تُرسل (الإرسال معطل).*»	الإرسال الفعلي غير نشط. راجع المشغّل.
«لم يتلقَّ المفوَّض له رسائل بريدي.»	تحقق من أن التفويض ساري المفعول ويشمل التطبيق المعني، وأن **حول البريد الالكتروني** مفعّل.
«توقف هاتفي عن تلقي الإشعارات الفورية.»	سجّل الخروج من تطبيق الهاتف المحمول ثم سجّل الدخول مجددًا، واسمح بالإشعارات.
«وصلت رسالة البريد بنص قديم.»	ربما تستخدم الأتمتة نصًا خاصًا بها بدلًا من استخدام قالبك. اسأل باني التطبيقات.

للتعمّق أكثر

لبُناة التطبيقات: التفاعلات والأتمتة [بناء التطبيقات] · للمشغّلين ومطوّري التكامل: تسليم الإشعارات: مرجع تقني

رخصتك وحدود خطتك

ما الذي يتطلّب رخصة

يلزم وجود رخصة لتفعيل **الإدارة**، حيث يبني فريقك التطبيقات ويهيّئ المنصة. ويُصدر هذه الرخصةَ مورّدُ أسس، ويثبّتها المشغّلون ويجدّدونها كما هو موضّح في تثبيت الرخصة وتجديدها.

أين ترى رخصتك

لا توجد في أسس شاشة تعرض رخصتك. وتفاصيلها لدى المورّد: ما تشمله، وحدودها، وتاريخ انتهائها. فاسأل المورّد، أو الجهة التي تشغّل النشر لديكم.

حين لا توجد رخصة

- **لا توجد رخصة سارية.** لا يُفتح أسس، ويرى المستخدمون صفحة خطأ فيها زر **إعادة المحاولة** بدل صفحة تسجيل الدخول. تواصل مع المورّد. وللمشغّلين: حين تُرفض الرخصة.
- **رخصة لا تشمل الإدارة.** لا تظهر قائمة **الإدارة**، ويؤدي فتح أي عنوان في الإدارة إلى صفحة «ليس لديك الصلاحية»، وتُرفض تغييرات تهيئة المنصة. ويواصل المستخدمون قراءة المُدخلات والعمل عليها كالمعتاد.

حدود الخطة `Since 1.10`

قد تحدّد خطتك عدد المُدخلات المسموح بها لمؤسستك. وتُحتسب المُدخلات في الكيانات التي بناها فريقك، ويُحتسب المُدخل المؤرشف بربع مُدخل.

- **التحذيرات.** في التثبيت المشترك، حين تبلغ مُدخلاتك 80% من الحد ثم حين تبلغه، يتلقى مسؤولو النظام إشعارًا في أسس ورسالة بالبريد الإلكتروني. ويذكر الإشعار العدد الذي يبدأ عنده رفض المُدخلات الجديدة: 10% فوق الحد، ما لم تسمح خطتك بتجاوزه.
- **تثبيت تطبيق.** يُرفض تثبيت الحزمة التي ستتجاوز بك ذلك العدد قبل كتابة أي شيء، برسالة توضّح ذلك.
- **ما يبقى متاحًا دائمًا.** قراءة المُدخلات وتعديلها وتصديرها.

ولإفساح المجال، أرشِف المُدخلات التي لم تعد تحتاج إليها أو احذفها. ولرفع الحد، تواصل مع المورّد.

المستخدمون من دليل شركتك

هذه الصفحة موجّهة إلى مسؤولي القاطن في المؤسسات التي تحفظ بيانات موظفيها في دليل للشركة: **Active Directory** على خوادم الشركة الخاصة، أو **Microsoft Entra ID** (المعروف سابقًا باسم Azure AD). وتشرح ما يفعله استيراد الدليل، والقرارات التي تتخذها، وما تسلّمه إلى المشغّل، وكيف تتحقق من النتيجة. ولا تشغّل الاستيراد بنفسك، إذ لا توجد له شاشة في **الإدارة**.

كيف يعمل

بدلًا من إضافة مئات الأشخاص يدويًا، يستطيع المشغّل جدولة استيراد يقرأ دليل شركتك ويُبقي أسس متزامنًا معه:

- **الأشخاص.** يصبح كل من له عنوان بريد إلكتروني في الدليل مستخدمًا في أسس، أو تُحدَّث بياناته إن كان موجودًا، وتطابق الأسماء وعناوين البريد الإلكتروني نظائرها في الدليل.
- **عضوية المجموعات.** لكل مجموعة أعددتها في أسس، يُضاف إليها الأشخاص الموجودون في مجموعة الدليل المقابلة لها.

يعمل الاستيراد وفق جدول يحدّده المشغّل، كل ساعة مثلًا، وتشمل كل عملية تشغيل المنضمّين الجدد وما طرأ من تغييرات.

مثال. لدى إدارة الموارد البشرية في الدليل مجموعة باسم *HR-Staff* تضم 20 شخصًا. تنشئ مجموعة **الموارد البشرية** في أسس وتربطها بـ *HR-Staff*. وبعد عملية التشغيل التالية، يصبح الأشخاص العشرون مستخدمين وأعضاء في **الموارد البشرية**. وعندما ينضم موظف موارد بشرية جديد إلى *HR-Staff* في الدليل، يظهر في أسس ضمن مجموعة **الموارد البشرية** بعد عملية التشغيل التي تلي انضمامه.

ما الذي لا يفعله الاستيراد

ضع ما يلي في الحسبان، إذ تبقى هذه المهام من مسؤوليتك:

- **لا يزيل أحدًا.** من يغادر الدليل، أو يغادر مجموعة في الدليل، يبقى في أسس وفي المجموعة؛ لذا أنهِ خدمة المغادرين بنفسك. راجع إنهاء خدمة شخص يغادر.
- **لا ينشئ مجموعات.** فهو يضيف الأعضاء إلى المجموعات التي أنشأتها وربطتها فقط.
- **لا يمنح وصولًا.** لا يحصل الأشخاص المستوردون على أي مستوى صلاحية على النظام ولا على أي أذونات حتى تمنحهم إياها، ويكون ذلك عادةً عبر مجموعاتهم.
- **لا يعيد المستخدمين المؤرشفين.** إذا كان شخص ما مؤرشفًا في أسس، يُبقيه الاستيراد مؤرشفًا.
- **يتخطى الأشخاص الذين ليس لهم عنوان بريد إلكتروني** في الدليل.

كيف يسجّل الأشخاص المستوردون الدخول

تُعلَّم حسابات الأشخاص المستوردين على أنها حسابات دليل؛ فهم **لا** يتلقون رسالة بريد إلكتروني لتعيين كلمة المرور، ولا يستطيعون تعيين كلمة مرور في أسس أو إعادة تعيينها، بل يسجّلون الدخول بحساب الشركة عبر **الدخول الموحّد**. لذا أعِدّ الدخول الموحّد قبل الاستيراد أو بالتزامن معه. راجع طرق تسجيل الدخول والدخول الموحّد.

قرّر ما الذي تستورده

اتفق مع المشغّل على ما يلي قبل عملية التشغيل الأولى؛ فهذه البنود تُدرَج في قائمة التسليم.

1. **أيّ دليل.** Active Directory على خوادم الشركة الخاصة، أو Microsoft Entra ID، أو كلاهما.
2. **أيّ الأشخاص.** الجميع، أو بعضهم فقط:
   - مع Active Directory، يمكن قصر الاستيراد على أعضاء مجموعة واحدة في الدليل.
   - مع Microsoft Entra ID، يمكن قصره على من يستوفون شرطًا، مثل *القسم هو المالية*.
3. **أيّ المجموعات تُزامَن.** أدرج مجموعات الدليل التي تريد إضافة أعضائها إلى مجموعات في أسس، وحدّد مجموعة أسس المقابلة لكلٍّ منها.
4. **كم مرة.** كل ساعة مثلًا، أو مرة كل ليلة.
5. **الأسماء.** تحقق مع المشغّل من طريقة مطابقة الاسم الأول واسم العائلة؛ فمع Active Directory، قد يعكس الإعداد القياسي موضعَي الاسم الأول واسم العائلة، لذا اطلب تصحيحه قبل عملية التشغيل الأولى.

إعداد المجموعات

لكل مجموعة في الدليل تريد مزامنتها:

1. **أنشئ مجموعة أسس**، مثل **الموارد البشرية**، من **الإدارة › المنظمة › مجموعات المستخدمين**. راجع إنشاء مجموعة.
2. **اربطها بمجموعة الدليل.** يجب أن تُعلَّم المجموعة بأنها مجموعة من الدليل، وأن تحمل معرّف مجموعة الدليل: اسمها المميّز (distinguished name) في Active Directory (مثل `CN=HR-Staff,OU=Groups,DC=example,DC=com`)، أو معرّف الكائن (object ID) في Microsoft Entra ID.

لا يتضمن نموذج المجموعة افتراضيًا حقولًا لهذا الربط، بل يضيفها أحد بُناة التطبيقات أو المشغّل مرة واحدة إلى كيان **مجموعات المستخدمين**، ثم تظهر في كل مجموعة. اطلب ذلك من المشغّل عند تسليمه القائمة.

3. **امنح المجموعة أذوناتها**، كي يحصل الأشخاص على ما يحتاجون إليه فور إضافتهم. ويجب أن تتضمن هذه الأذونات مستوى صلاحية على النظام لا يقل عن **مقيّد**. راجع الأذونات والوصول.

قائمة التسليم

انسخ هذا الجدول واملأه وأرسله إلى المشغّل. أما كلمات المرور والأسرار فأرسلها منفصلةً عبر قناة آمنة.

#	البند	قيمتك
A	**الدليل**	
A1	Active Directory، أو Microsoft Entra ID، أو كلاهما	
A2	Active Directory: عنوان الخادم، والجزء المطلوب قراءته من الدليل (القاعدة)	
A3	Active Directory: حساب للقراءة فقط يستطيع قراءة المستخدمين والمجموعات *(تُرسَل كلمة المرور منفصلةً)*	
A4	Microsoft Entra ID: معرّف الدليل (القاطن)	
A5	Microsoft Entra ID: تسجيل تطبيق له إذن من نوع **التطبيق** لقراءة جميع المستخدمين والمجموعات، مع معرّف العميل وسرّ العميل *(يُرسَل السر منفصلًا)*، وتاريخ انتهاء صلاحية السر	
B	**النطاق**	

#	البند	قيمتك
B1	استيراد الجميع، أو قصره على: مجموعة واحدة في الدليل (Active Directory) / شرط مثل القسم (Entra ID)	
B2	مجموعات الدليل المطلوب مزامنتها ← مجموعة أسس المقابلة لكلٍّ منها	
B3	إضافة حقول الربط بالدليل إلى كيان **مجموعات المستخدمين** (مطلوبة للبند B2)	نعم / أُنجز مسبقًا
C	**التشغيل**	
C1	جدول استيراد الأشخاص (كل ساعة مثلًا)	
C2	جدول استيراد عضوية المجموعات (يعمل بعد استيراد الأشخاص)	
C3	التحقق من مطابقة الأسماء (الاسم الأول واسم العائلة غير مقلوبين)	نعم / لا
C4	من يُبلَّغ عند فشل إحدى عمليات التشغيل	

يختلف تسجيل التطبيق في البند A5 عن التسجيل المستخدم للدخول الموحّد: فالاستيراد يقرأ الدليل بصورة مستقلة، دون أن يسجّل أحد الدخول، ولذلك يحتاج إلى أذونات من نوع التطبيق. أما أذونات Microsoft Graph المحدّدة فيختارها مسؤول Entra لديكم.

> **نصيحة**
>
> دوّن تاريخ انتهاء صلاحية سرّ العميل في Entra في تقويمك، إذ يتوقف الاستيراد عند انتهاء صلاحيته. أنشئ سرًّا جديدًا قبل ذلك التاريخ وأرسله إلى المشغّل.

التحقق من النتيجة

بعد عملية التشغيل الأولى:

1. افتح **الإدارة › المنظمة › المستخدمون** وتحقق من وجود الأشخاص المتوقعين، ومن صحة ترتيب أسمائهم.
2. افتح كل مجموعة متزامنة ضمن **مجموعات المستخدمين** وتحقق من أعضائها في تبويب **المستخدمين**.
3. اختر شخصًا مستوردًا واحدًا وتحقق من أذونات وصوله في **الإدارة › إدارة الوصول › أذونات وصول المستخدم**.
4. اطلب من أحد الأشخاص المستوردين تسجيل الدخول عبر الدخول الموحّد.

معلومات مفيدة

- **الدليل هو المرجع في الأسماء وعناوين البريد الإلكتروني.** إذا غيّرت اسم شخص مستورد في أسس، تعيده عملية التشغيل التالية إلى ما كان عليه. لذا غيّره في الدليل بدلًا من ذلك.
- **الأشخاص الموجودون أصلًا في أسس** يُطابَقون بعنوان البريد الإلكتروني (ومع Entra ID بمعرّفهم في الدليل أيضًا)، فتُحدَّث بياناتهم دون إنشاء حسابات مكررة.
- **إعادة تشغيل الاستيراد لا تضيف الأشخاص إلى المجموعة مرتين.**
- **أدلة Entra ID الكبيرة.** تُقرأ عضوية المجموعات من الصفحة الأولى فقط لقائمة المجموعات، ومن الصفحة الأولى فقط لقائمة أعضاء كل مجموعة، كما تُعيدها Microsoft. فإذا كنت تزامن مجموعات كثيرة أو مجموعات كبيرة جدًا، فاطلب من المشغّل التأكد من استيراد الجميع.

استكشاف الأخطاء وإصلاحها

ما تراه	ما الذي تتحقق منه
أحد الأشخاص مفقود.	ليس له عنوان بريد إلكتروني في الدليل، أو أنه خارج النطاق الذي اخترته (B1)، أو مؤرشف في أسس.
تبقى إحدى المجموعات فارغة.	المجموعة غير معلَّمة بأنها مجموعة من الدليل، أو أن معرّفها لا يطابق معرّف المجموعة في الدليل تمامًا، أو أن استيراد الأشخاص لم يُشغَّل بعد.
شخص غادر لا يزال في مجموعة.	الاستيراد لا يزيل الأشخاص أبدًا. أزِله بنفسك.
الاسم الأول واسم العائلة مقلوبان.	اطلب من المشغّل تصحيح مطابقة الأسماء (C3).
لا يستطيع الأشخاص المستوردون تسجيل الدخول.	الدخول الموحّد غير مُعَدّ لنطاقهم، أو أن حسابهم في الدليل لا يطابق عنوان البريد الإلكتروني في أسس.
لم يعد يظهر أشخاص جدد.	يفشل الاستيراد. ومع Entra ID، ربما انتهت صلاحية سرّ العميل. اطلب من المشغّل مراجعة سجلات الاستيراد.

للتعمّق أكثر

للمشغّلين: عمليات مزامنة الدليل · خادم الهوية ومزوّدو الهوية الخارجيون

طرق تسجيل الدخول والدخول الموحّد

تُخاطِب هذه الصفحة مسؤولي القاطن، وتشرح الطرق التي يسجّل بها المستخدمون دخولهم إلى أسس: ما يمكنك تفعيله بنفسك من **الإدارة**، وما يتطلّب تدخّل المشغّل. وتُختتم بدليل عملي متكامل، خطوة بخطوة، لإعداد الدخول الموحّد مع **Microsoft Entra ID** (المعروف سابقًا باسم Azure AD)، أو مع أي مزوّد هوية آخر يدعم OpenID Connect.

آلية العمل

يسجّل الجميع دخولهم من صفحة تسجيل الدخول نفسها، غير أنّ ما تعرضه هذه الصفحة يتوقّف على **النطاق**، أي عنوان الويب الذي يفتح منه المستخدمون أسس (مثل `portal.example.com`). ولكل نطاق إعدادات تسجيل دخول مستقلة؛ إذ تستطيع المؤسسة مثلًا إتاحة الدخول بحساب الشركة لموظفيها على عنوان الموظفين، بينما يدخل الشركاء الخارجيون بكلمة مرور على عنوان آخر.

ويمكن أن يتيح النطاق أيّ مزيج من الخيارات الآتية:

خيار تسجيل الدخول	ما يفعله المستخدمون	من يفعّله
كلمة المرور	يكتبون اسم المستخدم أو البريد الإلكتروني، ثم كلمة المرور.	أنت، لكل نطاق على حدة.
مفتاح المرور	يستخدمون بصمة الإصبع أو التعرّف على الوجه أو رمز PIN في الجهاز بدلًا من كلمة المرور.	تفعّل أنت مفاتيح المرور لكل نطاق، ثم ينشئ كل مستخدم مفتاح المرور الخاص به.
رمز العامل الثاني	يكتبون بعد كلمة المرور رمزًا لمرة واحدة يصلهم برسالة نصية أو بالبريد الإلكتروني أو عبر واتساب، أو يظهر في تطبيق مصادقة.	أنت، لكل نطاق (الرسالة النصية والبريد الإلكتروني). أمّا واتساب فيتوقّف على إعدادات المراسلة لديك. ويفعّل المستخدمون تطبيق المصادقة بأنفسهم.
الدخول الموحّد (SSO)	يختارون زرًّا مثل **تسجيل الدخول باستخدام Contoso**، ويسجّلون الدخول بحساب الشركة الذي لديهم أصلًا.	تُعدّه أنت مع المسؤول عن مزوّد الهوية في شركتك، ثم يربطه **المشغّل** بـ أسس.

مثال. تعتمد شركة Contoso على Microsoft Entra ID لجميع موظفيها؛ فيسجّل مسؤولها أسس في Entra، ويسلّم بيانات الاتصال إلى المشغّل، ثم يوقف تسجيل الدخول بكلمة المرور على نطاق الموظفين. ومنذ ذلك الحين، ينتقل الموظفون عند فتح البوابة مباشرةً إلى صفحة تسجيل الدخول في Microsoft، ثم يعودون إلى أسس وقد سُجّل دخولهم، وتتولّى قواعد الأمان الخاصة بـ Microsoft (مثل المصادقة متعددة العوامل في Entra) حماية الحساب.

تحديد طرق تسجيل الدخول على نطاق

لتغيير خيارات تسجيل الدخول لنطاق ما، عدّل مُدخل ذلك النطاق؛ إذ لا توجد شاشة مستقلة لإعدادات تسجيل الدخول.

1. افتح **الإدارة › التطبيقات › الكيانات**، ثم افتح كيان **نطاق**.
2. افتح النطاق الذي تريد تغييره. يتضمّن التثبيت الجديد نطاقًا واحدًا اسمه **Default Domain**، وتعرض قائمة **المضيف** فيه عناوين الويب التابعة له.
3. اختر **تعديل**، واضبط الخيارات المبيّنة أدناه، ثم اختر **حفظ**.

الحقل	عند تفعيله
السماح بتسجيل المستخدم	تعرض صفحة تسجيل الدخول نموذج اسم المستخدم وكلمة المرور.
دعم مفاتيح المرور `Since 1.6`	تعرض صفحة تسجيل الدخول **استخدام مفتاح المرور** ويستطيع المستخدمون إضافة مفاتيح مرور إلى حساباتهم.

الحقل	عند تفعيله
رسائل نصية للمصادقة الثنائية `Since 1.6`	يُطلب من المستخدمين بعد كتابة كلمة المرور إدخال رمز يصل إلى هواتفهم برسالة نصية.
البريد الإلكتروني للمصادقة الثنائية `Since 1.6`	يُطلب من المستخدمين بعد كتابة كلمة المرور إدخال رمز يصل إلى بريدهم الإلكتروني.
السماح بالتحقق بكلمة المرور `Since 1.8`	يستطيع من لا يملك وسيلة للتحقّق بعامل ثانٍ أن يؤكّد هويته بكلمة المرور قبل أن تُكشف له قيمة محمية. انظر كشف قيمة حساسة مقنَّعة [استخدام أسس › أمان الحساب وكشف القيم المحمية].

يسري التغيير عند تسجيل الدخول التالي على ذلك النطاق، ولا يؤدي إلى تسجيل خروج المستخدمين المسجّل دخولهم بالفعل.

> ⚠ **احتفظ بطريقة للدخول**
>
> لا توقف **السماح بتسجيل المستخدم** إلا بعد أن تختبر الدخول الموحّد بحساب حقيقي، وتتأكّد من قدرة مسؤول واحد على الأقل على الدخول من خلاله. فإن لم يبقَ على النطاق أي خيار دخول يعمل، تعذّر على الجميع الوصول إليه حتى يعيد المشغّل تفعيل أحد الخيارات.

تفاصيل تقنية

تُنسخ خيارات تسجيل الدخول للنطاق إلى خدمة تسجيل الدخول في كل مرة يُحفظ فيها مُدخل النطاق. ويُحدَّد النطاق المطبَّق على عملية تسجيل الدخول بحسب عنوان التطبيق الذي يسجّل المستخدم الدخول إليه؛ فهو النطاق الذي تتضمّن قائمة **المضيف** فيه ذلك العنوان. ولا يمكن أرشفة النطاقات التي ما زالت تستخدمها معارض أو تقارير.

خيارات العامل الثاني

يتطلّب العامل الثاني من المستخدم إثبات هويته مرة ثانية بعد كتابة كلمة المرور. وتعرض صفحة تسجيل الدخول جميع الطرق المتاحة له، وتُقدِّم أولًا الطريقة التي استخدمها في المرة السابقة على هذا الحساب. `Since 1.8` ويُحفظ هذا الاختيار لكل حساب، لا لكل متصفّح؛ فتظل لكل مستخدم طريقته الافتراضية الخاصة حتى إن تشارك مع آخرين حاسوبًا واحدًا.

- **تطبيق المصادقة.** يفعّله المستخدمون بأنفسهم من صفحة **الأمان** (**المصادقة الثنائية › تفعيل تطبيق المصادقة**). وبعد ذلك يُطلب منهم رمز في كل مرة، أيًّا كانت إعدادات النطاق. انظر أمان الحساب [استخدام أسس › أمان الحساب وكشف القيم المحمية].
- **رموز الرسائل النصية (SMS) والبريد الإلكتروني.** تُفعَّل لكل نطاق عبر **رسائل نصية للمصادقة الثنائية** و**البريد الإلكتروني للمصادقة الثنائية**. وعلى من يطلب رموزًا كثيرة في وقت قصير الانتظار بضع دقائق قبل طلب رمز جديد. ويتوقّف الرمز عن العمل إذا أُدخل خطأً مرات كثيرة، وعندئذٍ يستطيع المستخدم اختيار **إعادة إرسال الرمز**.
- **مفاتيح المرور.** عند تفعيل **دعم مفاتيح المرور**، يستطيع المستخدمون إضافة مفتاح مرور من صفحة **الأمان**، واستخدامه إمّا لتسجيل الدخول وإمّا خطوةً ثانية.

رموز واتساب `Since 1.10`

يستطيع أسس أيضًا إرسال رموز تسجيل الدخول عبر واتساب، ويظهر خيار واتساب عند تحقّق الشرطين معًا:

1. **أن تكون رموز الدخول عبر واتساب مُعدّة في مؤسستك.** ويُضبط ذلك ضمن إعدادات واتساب في إعدادات النظام لديك: ربط رقم واتساب للأعمال، وإدراج واتساب ضمن قنوات الرموز المسموح بها، وتوفير قالب رسالة معتمد لرمز تسجيل الدخول. ولا توجد في 1.10 شاشة مخصّصة لهذه الإعدادات. انظر كتلة إعدادات واتساب.

2. **أن يكون للمستخدم رقم هاتف موثّق** في حسابه.

> ⚠ **واتساب يفعّل العامل الثاني لكل من لديه هاتف موثّق**
>
> لا يعتمد واتساب على مفتاح **رسائل نصية للمصادقة الثنائية**. فمتى أُعدّت رموز واتساب، **يُطلب رمز عند الدخول من كل من لديه رقم هاتف موثّق**، حتى على نطاق أُوقف فيه الخياران **رسائل نصية للمصادقة الثنائية** و**البريد الإلكتروني للمصادقة الثنائية** معًا.

وحين تتاح للمستخدم الرسائل النصية وواتساب معًا، تحدّد إعدادات واتساب لديك أيّهما يُعرض أولًا. ولا يصلح رمز واتساب إلا عبر واتساب، ولا يصلح رمز الرسالة النصية إلا عبر الرسائل النصية. وإن تعذّر استخدام واتساب في عملية دخول ما، فلن يُسمح للمستخدم بالدخول دون عامل ثانٍ أبدًا؛ إذ يتعذّر على من كانت طريقته الوحيدة واتساب تسجيل الدخول حتى يعود واتساب إلى العمل.

وتظهر الرسائل التي لم تُرسَل في سجل رسائل واتساب. انظر قناة واتساب.

> ⓘ **للتعمّق أكثر**
>
> للمشغّلين: خادم الهوية: العوامل الثانية والرموز

إعداد الدخول الموحّد مع Microsoft Entra ID

يتيح الدخول الموحّد للمستخدمين تسجيل الدخول بالحساب الذي تديره شركتك أصلًا في Microsoft Entra ID، ويتطلّب إعداده تعاون الأطراف الآتية:

من	ماذا يفعل
أنت (مسؤول القاطن)	تحدّد القواعد، وتملأ ورقة العمل، وتختار النطاقات، وتُجري الاختبار.
مسؤول Entra لديك (وكثيرًا ما تكون أنت)	يسجّل أسس بوصفه تطبيقًا في Microsoft Entra، وينشئ سرّ عميل.
المشغّل	يضيف المزوّد إلى خدمة تسجيل الدخول في أسس مستعينًا بورقة العمل. ولا يمكن تنفيذ ذلك في 1.10 من **الإدارة**.

قبل أن تبدأ

- تحتاج إلى إذن الوصول إلى مركز إدارة Microsoft Entra مع إذن بتسجيل التطبيقات، أو إلى الاستعانة بشخص يملك هذا الإذن وهذا الإذن.
- تحتاج إلى جهة اتصال لدى مشغّل أسس، وإلى وسيلة آمنة لإرسال سرّ إليه، مثل مدير كلمات المرور أو رسالة مشفّرة. لا ترسل سرّ العميل في بريد إلكتروني عادي أو في محادثة.
- حدّد ما سيحدث للمستخدمين الذين لديهم حساب في أسس أصلًا، وللمستخدمين الجدد، كما هو موضّح في الخطوة 1.

الخطوة 1: حدّد القواعد

اتفق مع المشغّل على ما يلي قبل البدء بأي تسجيل؛ إذ تُدوَّن هذه القرارات في الجزء C من ورقة العمل.

1. **اسم قصير للمزوّد.** استخدم أحرفًا لاتينية صغيرة فقط، مثل `entra` . يصبح هذا الاسم جزءًا من عنوان تسجيل الدخول المسجَّل في Entra، لذا يقتضي تغييره لاحقًا تحديث Entra أيضًا.

2. **نص الزر**، مثل *Contoso*. تعرض صفحة تسجيل الدخول **تسجيل الدخول باستخدام Contoso** تحت عبارة **تسجيل الدخول إلى حسابك باستخدام**. ويمكنك تقديم عنوان صورة شعار بدلًا من النص.
3. **النطاقات** التي يظهر فيها الزر. حدّدها بالاسم و**المضيف**.
4. **المستخدمون الذين لديهم حساب أصلًا.** يتعرّف أسس على المستخدم من عنوان البريد الإلكتروني الذي يوفّره حسابه في Entra. اختر أحد الخيارات الآتية:

- **استُوردوا من Entra عبر مزامنة الدليل.** يُتعرَّف عليهم تلقائيًا دون أي خطوة إضافية. انظر مزامنة الدليل.
- **اطلب منهم ربط حساباتهم مرة واحدة.** في أول مرة يستخدمون فيها الزر، يطلب أسس كلمة مرورهم الحالية ويعرض **ربط حسابي**، وبعد ذلك يسجّلون دخولهم مباشرةً باستخدام الزر.
- **لا هذا ولا ذاك.** يُرفض دخول من لديهم حساب بكلمة مرور عند استخدامهم الزر.

5. **المستخدمون الذين ليس لديهم حساب بعد.** إمّا أن ترفض دخولهم (فتنشئ أنت حساباتهم أولًا)، وإمّا أن **تنشئ حساباتهم تلقائيًا**. وإن اخترت الإنشاء التلقائي، فحدّد **مجموعة المستخدمين** و**المساحة** اللتين ينضمّ إليهما المستخدمون الجدد، ويمكنك اختياريًا وضع قاعدة مثل «عناوين البريد الإلكتروني المنتهية بـ @contoso.com فقط».
6. **تحديث الملفات الشخصية.** اختر ما إذا كان أسس سينسخ اسم المستخدم وبريده الإلكتروني من Entra عند كل تسجيل دخول، أم عند إنشاء الحساب فقط.

الخطوة 2: احصل على عنوان تسجيل الدخول

يحتاج Entra إلى معرفة العنوان الذي يعيد إليه المستخدمين بعد تسجيل دخولهم، ويتكوّن هذا العنوان من **عنوان خادم تسجيل الدخول** واسم المزوّد:

```
https://<sign-in server address>/ext-auth/<provider name>/redirect
```

مثال: `https://identity.contoso.com/ext-auth/entra/redirect`.

اطلب عنوان خادم تسجيل الدخول من المشغّل، أو تحقّق منه بنفسك: افتح صفحة تسجيل الدخول وانظر إلى شريط العنوان في المتصفّح، فهو يعرض عنوان خادم تسجيل الدخول. استخدم هذا المضيف كما هو تمامًا، مع `https://` ودون شرطة مائلة في النهاية.

الخطوة 3: سجّل أسس في Microsoft Entra ID

تُجري Microsoft تغييرات على مركز الإدارة من حين لآخر؛ فإن لم تطابق إحدى التسميات أدناه ما تراه، فارجع إلى دليل Microsoft لتسجيل التطبيقات. وتَرِد تسميات Entra هنا بالإنجليزية كما تظهر في واجهته.

1. في مركز إدارة Microsoft Entra، افتح **App registrations** واختر **New registration**.
2. امنح التطبيق اسمًا مألوفًا للمستخدمين، مثل *بوابة أسس*.
3. تحت **Supported account types**، اختر **Accounts in this organizational directory only**، إلا إذا كنت تقصد السماح لحسابات من مؤسسات أخرى بتسجيل الدخول.
4. تحت **Redirect URI**، اختر المنصّة **Web** والصق العنوان الذي حصلت عليه في الخطوة 2. لا تختر *Single-page application*.
5. اختر **Register**، ثم انسخ من صفحة النظرة العامة **Application (client) ID** و**Directory (tenant) ID** إلى ورقة العمل.
6. افتح **Certificates & secrets**، واختر **New client secret**، وحدّد مدة الصلاحية. انسخ قيمة السرّ (**Value**) فورًا، لأن Entra لا يعرضها إلا مرة واحدة، ودوّن تاريخ انتهاء صلاحيته.

7. افتح **API permissions**، وتأكّد من وجود الأذونات المفوَّضة `openid` و`profile` و`email` و`User.Read` من Microsoft Graph. وإن كانت مؤسستك تشترط ذلك، فاختر **Grant admin consent**.

> **نصيحة**
>
> أضف تاريخ انتهاء صلاحية السرّ إلى تقويمك؛ فعند انتهائه يتوقّف الدخول الموحّد عن العمل. أنشئ سرًّا جديدًا في Entra قبل ذلك التاريخ، وأرسله إلى المشغّل بالطريقة نفسها.

الخطوة 4: سلّم ورقة العمل إلى المشغّل

أرسل ورقة العمل بعد إكمالها إلى المشغّل، وأرسل سرّ العميل منفصلًا عبر قناتك الآمنة. يضيف المشغّل المزوّد إلى خدمة تسجيل الدخول ويربطه بنطاقاتك، ويسري ذلك اعتبارًا من تسجيل الدخول التالي، دون حاجة إلى إعادة التشغيل.

> **للتعمّق أكثر**
>
> للمشغّلين: خادم الهوية: إضافة مزوّد هوية خارجي

الخطوة 5: اختبر الإعداد

1. افتح البوابة على أحد النطاقات المختارة في نافذة تصفّح خاصة.
2. تحقّق من أن صفحة تسجيل الدخول تعرض **تسجيل الدخول إلى حسابك باستخدام** ومعها الزر الذي حدّدته، مثل **تسجيل الدخول باستخدام Contoso**.
3. اختر الزر، وسجّل الدخول بحساب Entra تجريبي، وتأكّد من عودتك إلى أسس وقد سُجّل دخولك بهوية الشخص الصحيح.
4. اختبر الحالات التي اخترتها في الخطوة 1: استخدم حسابًا قائمًا (ينبغي أن يُتعرَّف عليه، أو أن يُطلب من صاحبه ربطه مرة واحدة)، وحساب شخص جديد تمامًا (ينبغي أن يحصل على حساب في المجموعة والمساحة المختارتين، أو أن يُرفض دخوله).
5. سجّل الخروج، وتحقّق من تسجيل خروجك من Microsoft أيضًا.

إذا أخفق أيّ من هذه الاختبارات، فانظر استكشاف الأخطاء وإصلاحها.

الخطوة 6 (اختيارية): اجعل الدخول الموحّد الطريق الوحيد للدخول

عندما يصبح جميع مستخدمي النطاق قادرين على تسجيل الدخول عبر Entra، يمكنك إيقاف الخيارات الأخرى:

1. عدّل النطاق (انظر تحديد طرق تسجيل الدخول على نطاق)، وأوقف **السماح بتسجيل المستخدم** و**دعم مفاتيح المرور**.
2. `Since 1.10` إذا أصبح الدخول الموحّد الخيار الوحيد على ذلك النطاق، ولم يكن في صفحة تسجيل الدخول لديك رابط لإنشاء حساب، فإن المستخدمين يتخطّون صفحة تسجيل الدخول كليًّا وينتقلون مباشرةً إلى Microsoft، فلا تظهر الصفحة ولا رابط **إلغاء** فيها. ويستطيع المشغّل إيقاف هذا التخطّي إن كنت تفضّل عرض الصفحة في كل مرة، كما أن وجود رابط لإنشاء حساب يُبقي الصفحة ظاهرة؛ انظر إعدادات المنظمة.

مزوّدو هوية آخرون

تنطبق الخطوات نفسها على مزوّدي الهوية الآخرين الذين يدعمون تسجيل الدخول عبر OpenID Connect أو OAuth 2.0 بسرّ عميل، مثل Okta أو Google Workspace أو الهوية الرقمية الوطنية. ولكل مزوّد مصطلحاته، غير أنّك تجمع العناصر نفسها: عنوانَي تسجيل الدخول والرموز لدى المزوّد، ومعرّف العميل وسرّه، ونطاقات الإذن (scopes) المطلوبة، وعنوان الملف الشخصي للمستخدم، وحقول الملف الشخصي التي تحمل معرّفًا ثابتًا والبريد الإلكتروني والاسم. وسجّل عنوان إعادة التوجيه نفسه من الخطوة 2.

ورقة عمل الدخول الموحّد

انسخ هذا الجدول واملأه وأرسله إلى المشغّل، وأرسل سرّ العميل منفصلًا.

#	البند	قيمتك
A	**خادم تسجيل الدخول**	
A1	عنوان خادم تسجيل الدخول (من المشغّل)	`https://`
A2	عنوان إعادة التوجيه المسجَّل في Entra	`https://<A1>/ext-auth/<C1>/redirect`
B	**من Microsoft Entra ID**	
B1	معرّف الدليل (Directory (tenant) ID)	
B2	معرّف التطبيق (Application (client) ID)	
B3	سرّ العميل	*(يُرسَل منفصلًا)*
B4	تاريخ انتهاء صلاحية سرّ العميل	
B5	الأذونات الممنوحة (`openid profile email User.Read`)	نعم / لا
B6	للحسابات التي ليس لها صندوق بريد: هل يُستخدم اسم تسجيل الدخول (user principal name) بريدًا إلكترونيًا؟	نعم / لا
C	**قراراتك**	
C1	اسم المزوّد (بأحرف صغيرة، مثل `entra`)	
C2	نص الزر أو عنوان صورة الشعار	
C3	النطاقات التي يظهر فيها الزر (الاسم والمضيف)	
C4	الحسابات القائمة: مستوردة بمزامنة الدليل / ربط لمرة واحدة بكلمة المرور / لا هذا ولا ذاك	
C5	المستخدمون الجدد: رفض / إنشاء تلقائي	
C6	عند الإنشاء التلقائي: مجموعة المستخدمين، والمساحة، وأي قاعدة (مثل نطاق البريد الإلكتروني)	
C7	تحديث الاسم والبريد الإلكتروني من Entra عند كل تسجيل دخول؟	نعم / لا
C8	اختياري: صياغتك الخاصة لرسائل الخطأ	
C9	بعد الاختبار، إيقاف كلمات المرور على هذه النطاقات؟	نعم / لا

تجربة المستخدمين مع الدخول الموحّد

صفحة الأمان لمستخدمي الدخول الموحّد `Since 1.8`

يدير المستخدمون الذين يسجّلون دخولهم عبر مزوّد هوية كلمةَ مرورهم وعاملهم الثاني لدى ذلك المزوّد، لا في أسس؛ لذا يرون في صفحة **الأمان**، بدلًا من تبويبَي المصادقة الثنائية و**مفاتيح المرور**، الرسالة الآتية: *«تتم إدارة المصادقة الثنائية ومفاتيح المرور لهذا الحساب عبر موفّر الهوية الخاص بمؤسستك.»* كما يتعذّر عليهم تغيير كلمة مرور أسس أو إعادة تعيينها.

ولا يطلب أسس من مستخدمي الدخول الموحّد رمز العامل الثاني الخاص به. فإن أردت تفعيل عامل ثانٍ لهم، فأعِدّه لدى مزوّد الهوية لديك (مثل الوصول المشروط Conditional Access في Microsoft Entra).

تسجيل الخروج

عند تسجيل الخروج من أسس، يُحال المستخدمون أيضًا إلى صفحة تسجيل الخروج لدى مزوّد الهوية، فيُسجَّل خروجهم منه كذلك.

فتح مزوّد محدّد مباشرةً `Since 1.10`

يمكن لرابط يؤدي إلى أسس أن يحدّد المزوّد المطلوب، فيتخطّى المستخدمون خطوة اختيار المزوّد وينتقلون إليه مباشرةً. ويفيد ذلك مثلًا عند وضع الرابط في صفحة على الشبكة الداخلية للمؤسسة. ويدعم رابط تسجيل الدخول في البوابة هذه الميزة: انظر تسجيل الدخول واختيار مساحة [استخدام أسس]. ويستخدم الرابط اسم المزوّد (C1 في ورقة العمل)، لا نص الزر: فإن لم يطابق الاسم مزوّدًا على ذلك النطاق، ظهرت صفحة تسجيل الدخول المعتادة.

معلومات مفيدة

رابط الإلغاء في صفحة تسجيل الدخول `Since 1.4`

تحتوي صفحة تسجيل الدخول على رابط **إلغاء** يُنهي عملية تسجيل الدخول ويعيد المستخدم إلى التطبيق الذي جاء منه، أي إلى الصفحة الرئيسية في حالة بوابة الويب. وإذا بقيت صفحة تسجيل الدخول دون تفاعل مدة 10 دقائق، فإنها تُلغي عملية تسجيل الدخول بالطريقة ذاتها.

روابط إعادة تعيين كلمة المرور `Since 1.4`

عندما يختار المستخدم **هل نسيت كلمة المرور؟**، يرسل إليه أسس رابط إعادة تعيين بالبريد الإلكتروني:

- يظل الرابط صالحًا 24 ساعة افتراضيًا، ويستطيع المشغّل تغيير هذه المدة.
- يؤدي تكرار الطلب إلى إرسال **رابط جديد وإبطال الرابط القديم**، فلا يصلح إلا أحدث رابط.
- لا يحتفظ أسس إلا ببصمة مُعمّاة للرابط، فلا يوجد الرابط الصالح إلا في البريد، وتعرض نسخة الرسالة في سجل البريد `[redacted]` مكانه. انظر رموز إعادة التعيين ورموز API خارج سجل البريد.
- لا يستطيع مستخدمو الدخول الموحّد إعادة تعيين كلمة مرور أسس.

وبعد الترقية إلى إصدار يتضمّن هذه الحماية، تتوقّف روابط إعادة التعيين المرسلة قبل الترقية عن العمل، ويكفي أن يطلب المستخدمون رابطًا جديدًا.

الحسابات المقفلة والمعطّلة

يؤدي تكرار إدخال كلمة مرور خاطئة إلى قفل الحساب مؤقتًا، ولا يستطيع المستخدم المعطَّل تسجيل الدخول بأي طريقة. وللحماية من تخمين كلمات المرور، تحدّ صفحات كلمة المرور أيضًا من عدد المحاولات الواردة من مكان واحد خلال وقت قصير: فمن يبلغ هذا الحد يرى رسالة خطأ، ويستطيع المحاولة مجددًا بعد نحو 15 دقيقة.

سجل تسجيل الدخول

يسجّل أسس كل محاولة لتسجيل الدخول، الناجحة منها والفاشلة، بما في ذلك طريقة الدخول وما إذا استُخدم عامل ثانٍ. ويستطيع المستخدمون مراجعة محاولات تسجيل دخولهم الأخيرة من صفحة **الأمان**. انظر الجلسات ومحاولات تسجيل

الدخول [استخدام أسس › أمان الحساب وكشف القيم المحمية].

عندما تتشارك مؤسستك نشرًا واحدًا مع مؤسسات أخرى `Since 1.10`

في النشر الذي يخدم عدة مؤسسات، تملك كل مؤسسة خدمة تسجيل دخول مستقلة، لها عنوان تسجيل دخول وحسابات وجلسات ومزوّدون خاصون بها، ولا يظهر أيّ مما تُعدّه لمؤسسة أخرى. وإليك أمورًا قد تلاحظها:

- **المسؤول الأول** في المؤسسة الجديدة يتلقّى، عند تفعيل المؤسسة، رسالة بريد إلكتروني لتعيين كلمة مروره، ويعيده الرابط إلى عنوان المؤسسة نفسها.
- **علامتك التجارية** تظهر في صفحات تسجيل الدخول، وفي رسائل رموز الدخول، وفي تطبيقات المصادقة، إذا سُجّلت مؤسستك بعلامة تجارية. انظر العلامة التجارية لكل قاطن.
- **مطالبات مفتاح المرور** تعرض اسم العرض الخاص بمنظمتك.
- **أثناء الصيانة**، كأن يستعيد المشغّل نسخة احتياطية أو ينقل مؤسستك، يتعذّر على الجميع تسجيل الدخول، ويرى المستخدمون خطأً مؤقتًا حتى تنتهي الصيانة.

استكشاف الأخطاء وإصلاحها

ما تراه	ما يجب التحقق منه
لا يظهر الزر في صفحة تسجيل الدخول.	النطاق الذي فتحته ليس من النطاقات المرتبطة بالمزوّد (C3)، أو لم يفعّل المشغّل المزوّد بعد. قارن العنوان في المتصفّح بقائمة **المضيف** للنطاق.
تعرض Microsoft خطأً متعلقًا بعنوان إعادة التوجيه (مثل *AADSTS50011*).	عنوان إعادة التوجيه في Entra لا يطابق A2 تمامًا. تحقّق من `https`، والمضيف، واسم المزوّد، وعدم وجود شرطة مائلة في النهاية. ويجب أن يكون مسجّلًا تحت المنصّة **Web**.
يعود المستخدمون إلى صفحة تسجيل الدخول وتظهر الرسالة "Something went wrong during the login, please try again later!"	غالبًا ما تكون صلاحية سرّ العميل قد انتهت، أو يكون قد نُسخ خطأً، أو يكون أحد الأذونات ناقصًا. اطلب من المشغّل مراجعة سجل خدمة تسجيل الدخول لمعرفة السبب، وإضافة صياغتك الخاصة لهذا الخطأ إن أردت (C8).
يُرفض دخول مستخدم لديه حساب قائم.	حسابه في أسس يحمل البريد الإلكتروني نفسه، لكنه لم يُربط بعد. وربط الحسابات غير نشط. فعّل «الربط لمرة واحدة بكلمة المرور» (C4)، أو استورد المستخدم من Entra.
يُرفض دخول شخص جديد.	الإنشاء التلقائي للحسابات غير نشط، أو أن الشخص لا يستوفي قاعدتك (C5-C6).
يسجّل المستخدمون الجدد دخولهم لكن دون أي إذن وصول.	تحقّق من مجموعة المستخدمين والمساحة المختارتين للحسابات الجديدة (C6)، ومن أذونات المجموعة.
لا يستطيع أحد تسجيل الدخول بعد أن أوقفت كلمات المرور.	إن كنت ما زلت مسجّل الدخول، فأعِد تفعيل **السماح بتسجيل المستخدم** بنفسك، وإلا فاطلب من المشغّل إعادة تفعيله لذلك النطاق. ثم اختبر الدخول الموحّد من جديد.
تعذّر على شخص تسجيل الدخول على حاسوب مشترك بعد إزالة حساب شخص آخر. `Since 1.10`	لا حاجة إلى أي إجراء، فتسجيل الدخول صار يستبدل الجلسة القديمة تلقائيًا.
أصبح الجميع فجأةً مطالبين بإدخال رمز.	أُعدّت رموز واتساب، فأصبح الرمز مطلوبًا من كل من لديه هاتف موثّق. انظر رموز واتساب.

للتعمّق أكثر

للتعمّق أكثر

للمشغّلين: خادم الهوية والمزوّدون الخارجيون · لمطوّري التكامل: المصادقة OAuth [التكامل والتوسعة] · للمستخدمين النهائيين: أمان الحساب [استخدام أسس › أمان الحساب وكشف القيم المحمية]

إدارة الأذونات

استعن بهذا الدليل حين تحتاج إلى منح فريق وصولًا إلى جزء من أسس، أو تغيير ما يستطيع فعله، أو سحب الوصول منه. وتستخدم الأمثلة قسمًا للموارد البشرية: مجموعة **الموارد البشرية** ودور **مدير الموارد البشرية**. ولفهم طريقة عمل الوصول عمومًا، اقرأ الأذونات والوصول.

قبل أن تبدأ

- تحتاج إلى مستوى **إدارة** على النظام لتظهر لك **الإدارة › إدارة الوصول**.
- ما لم يكن مستواك على النظام «إدارة»، فلا يمكنك منح مستويات تتجاوز مستواك.
- امنح الوصول للمجموعات والأدوار بدلًا من الأفراد؛ فذلك أيسر في المراجعة، ويجعل وصول الأشخاص يتبع عضويتهم حين ينتقلون بين الفرق.

مستويات الوصول

من الأدنى إلى الأعلى:

- **مقيّد** – لا يتيح شيئًا بمفرده؛ إذ يُثبت أن الشخص عضو، فيسري ما تمنحه له من وصول في مواضع أخرى. ويحتاج كل شخص إلى هذا المستوى على الأقل على النظام.
- **عرض** – رؤية تصميم الوحدة أو الكيان، وفتح المعارض والصفحات والتقارير التي تمت مشاركتها معه.
- **مطور** – بناء التصميم وتغييره، دون رؤية المُدخلات.
- **تعديل** – كل ما يتيحه مستوى «مطور»، إضافةً إلى استعراض المُدخلات وفتحها وتغييرها في الإدارة.
- **إدارة** – تحكّم كامل في المنصة، على مستوى النظام فقط.

مستوى وصول الشخص هو أعلى مستوى تمنحه إياه منحُه كافة: المباشرة، والمكتسبة عبر كل مجموعة ودور ووحدة تنظيمية ينتمي إليها. ولا تسحب منحةٌ وصولًا تمنحه منحةٌ أخرى. ولكي يفتح الشخص مُدخلات كيانٍ في **الإدارة** – ولو مُدخلًا واحدًا – يحتاج إلى **تعديل**؛ فمستوى «عرض» لا يكفي.

امنح مجموعة مستوى على النظام

1. افتح **الإدارة › إدارة الوصول › أذونات المدير**.
2. اختر تبويب **المجموعات**، ثم اختر **إضافة**.
3. في **حدد مجموعة للإضافة**، اختر المجموعة، مثل مجموعة تضمّ جميع الموظفين.
4. في **حدد مستوى الصلاحية**، اختر المستوى – وهو عادةً **مقيّد** – ثم اختر **تأكيد**.

امنح مجموعة وصولًا إلى وحدة أو كيان بيانات

1. تأكّد من أن للمجموعة مستوى على النظام (راجع ما سبق)؛ إذ لا تظهر في القائمة إلا هذه المجموعات.
2. افتح الوحدة (**الإدارة › التطبيقات › الوحدات**) أو كيان البيانات (**الإدارة › التطبيقات › الكيانات**).
3. افتح تبويب **الأذونات**، وانتقل إلى **المجموعات**.

4. في صف المجموعة، اختر **مستوى الصلاحية** – **عرض** أو **مطور** أو **تعديل** – ثم أكّد. امنح مثلًا مجموعة **الموارد البشرية** مستوى **تعديل** على كيان الموظفين.

الوصول إلى وحدة يشمل كل كيان بداخلها. ولا يمكنك منح المجموعة على الكيان مستوى أدنى من مستواها على الوحدة.

امنح مجموعة وصولًا إلى معرض أو صفحة أو تقرير أو خدمة

1. افتح **الإدارة › إدارة الوصول › أذونات وصول المجموعة**.
2. في **اختر المجموعة**، اختر المجموعة.
3. اختر **إضافة إذن**، ثم اختر في **الكائن** المعرض أو الصفحة أو التقرير أو الخدمة.
4. إذا كان الكائن خدمة، فاختر **جمهور الخدمة** (يستطيعون تقديمها) أو **المتابِعين** (يرون كل طلباتها).
5. احفظ.

إضافة مجموعة إلى معرض أو صفحة أو تقرير تحوّله إلى الوضع **مقيّد**: فلا يفتحه إلا الأشخاص والمجموعات المدرَجون في قائمته.

> ⚠ **مشكلة معروفة: قد لا يظهر المعرض في الشريط الجانبي عند منح إذن الوصول إليه من هنا**
>
> عند منح مجموعة أو مستخدم إذن الوصول إلى معرض من **أذونات وصول المجموعة** أو **أذونات وصول المستخدم**، قد لا يظهر المعرض (ووحدته) في الشريط الجانبي لديهما إلا بعد إعادة فتح المعرض في مصمّم المعرض. ولإظهاره، امنح إذن الوصول من نافذة **الأذونات** الخاصة بالمعرض نفسه بدلًا من ذلك، أو افتح المعرض مرة واحدة في مصمّم المعرض (دون الحاجة إلى الحفظ). وقد يلزم أن يُحدّث المستخدم الصفحة ليظهر له المعرض.

غيّر الوصول أو احذفه

- **مستوى النظام:** في **أذونات المدير**، غيّر **مستوى الصلاحية** في الصف، أو اختر أيقونة سلة المهملات لحذفه، ثم أكّد.
- **وحدة أو كيان:** في تبويب **الأذونات** الخاص بالوحدة أو الكيان، غيّر **مستوى الصلاحية** ثم أكّد؛ وأعِده إلى **مقيّد** لسحب الوصول الممنوح هناك.
- **معرض أو صفحة أو تقرير أو خدمة:** في **أذونات وصول المجموعة** أو **أذونات وصول المستخدم**، عدّل الصف أو احذفه.

حذف المنحة يزيلها، لكنه لا يمنع الشخص من الوصول: إذ يحتفظ بأي وصول ما زال يحصل عليه عبر مجموعة أخرى أو دور أو مستوى النظام. ولمعرفة مصدر وصول شخص ما، افتح **أذونات وصول المستخدم**، واختر الشخص، ثم اقرأ **نوع الإذن** و**مكتسبة عن طريق**.

احمِ الحقول الحسّاسة

يستطيع باني التطبيق أن يضبط حقلًا مثل **الراتب** على أنه **حساس** في مصمّم الكيان (راجع الحقول الحسّاسة [بناء التطبيقات › حماية حقل]). فتُحجب قيمته عندئذ – وتظهر بالشكل `****` مع أيقونة قفل – عن كل من لا يملك منحة حقل حسّاس، بمن فيهم أصحاب مستوى «إدارة». ولا ترسل المنصة القيمة المحجوبة إلى أجهزتهم إطلاقًا.

للسماح لدور مدير الموارد البشرية برؤية الرواتب:

1. افتح **الإدارة › إدارة الوصول › الأذونات الحساسة**.
2. أضِف منحة: اختر مجموعة دور مدير الموارد البشرية، واختر حقل **الراتب** نطاقًا لها. ويمكنك أيضًا تحديد تاريخ انتهاء.
3. احفظ.

يرى أصحاب المنحة أيقونة عين بدلًا من القفل، وحين يختارونها يُطلب منهم تأكيد هويتهم قبل أن تظهر القيمة. وتجد الإجراء الكامل، بما في ذلك المنح المحدّدة بمدة، وتبويبات كل مستخدم وكل مجموعة، في الأذونات الحساسة.

مواضيع ذات صلة

- اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط
- الأذونات والوصول
- إدارة الأدوار

اجعل مجموعة الموارد البشرية ترى طلبات الموارد البشرية فقط

هذا الدليل موجّه إلى مسؤولي القاطن، وستضبط فيه الإعدادات بحيث يرى فريق الموارد البشرية كل طلب يُقدَّم عبر خدمات الموارد البشرية – كطلبات الإجازة وشهادات الراتب وغيرها – دون أن يطّلع على الطلبات المقدَّمة عبر خدمات أي قسم آخر.

كيف تُحدَّد رؤية الطلبات

لا تحدّد مستويات الوصول من يرى الطلب، بل يُحدَّد ذلك لكل **خدمة** على حدة:

من	ما يراه	أين يراه
مقدّم الطلب	طلباته هو	**الصادر**
مالكو خطوة في سير العمل	الطلبات التي تصل إلى خطوة يملكونها هم أو تملكها مجموعتهم	**الوارد**
المتابِعون	كل طلبات تلك الخدمة	**المتابعة**
جمهور الخدمة	الخدمة نفسها، ليتمكّنوا من تقديمها	**دليل الخدمات**

لذا فإن «ترى الموارد البشرية طلبات الموارد البشرية فقط» تعني إدراج مجموعة الموارد البشرية ضمن **المتابِعين** في كل خدمة من خدمات الموارد البشرية دون سواها. وبما أنك تضبط المراقبين لكل خدمة على حدة، تبقى طلبات الأقسام الأخرى تلقائيًا بعيدة عن نظر فريق الموارد البشرية.

> **ملاحظة**
>
> تبقى لمستويات الوصول أهميتها في موضع واحد: إذ يستطيع كل من لديه **تعديل** أو **إدارة** على مستوى النظام قراءة مُدخلات كل الخدمات في **الإدارة**. لذا أبقِ فريق الموارد البشرية على **مقيّد** أو **عرض** على مستوى النظام.

قبل أن تبدأ

- تحتاج إلى مستوى **إدارة** على النظام.
- يجب أن تكون خدمات الموارد البشرية موجودة مسبقًا؛ فتصميم الخدمة من مهام بُناة التطبيقات، أما أنت فتحدّد من يراقبها ومن يستطيع تقديمها إن أردت.
- مجموعة **الموارد البشرية** موجودة وتضمّ أعضاء فريق الموارد البشرية. راجع إدارة المجموعات.
- لكل عضو في فريق الموارد البشرية مستوى **مقيّد** على الأقل على النظام. راجع امنح الجميع مستوى أساسيًا.

الخطوة 1: اجعل مجموعة الموارد البشرية مراقبًا لكل خدمة من خدماتها

1. افتح **الإدارة › إدارة الوصول › أذونات وصول المجموعة**.
2. في **اختر المجموعة**، اختر **الموارد البشرية**.
3. في تبويب **أذونات المجموعة**، اختر **إضافة إذن**.
4. في **الكائن**، اختر أول خدمة من خدمات الموارد البشرية، مثل **طلب إجازة**.

5. في **مستوى الوصول**، اختر **المتابِعين**.
6. احفظ.
7. كرّر ذلك لكل خدمة أخرى من خدمات الموارد البشرية.

يرى فريق الموارد البشرية الآن كل طلبات هذه الخدمات في **المتابعة**، بما في ذلك الطلبات المقدَّمة قبل إضافتهم.

الخطوة 2: تحقّق من أن الموارد البشرية لا تراقب أي خدمة أخرى

1. وأنت ما زلت في **أذونات وصول المجموعة** لمجموعة **الموارد البشرية**، راجع القائمة.
2. إذا تضمّنت القائمة خدمةً لا تتبع الموارد البشرية – مثل مكتب خدمات تقنية المعلومات – فاحذف ذلك الصف.
3. افتح **الإدارة › إدارة الوصول › أذونات المدير**، وتحقّق من أن مستوى مجموعة الموارد البشرية هو **مقيّد** أو **عرض**، وليس **تعديل** أو **إدارة**.

الخطوة 3 (اختيارية): حدّد من يستطيع تقديم كل خدمة من خدمات الموارد البشرية

قد تكون الخدمة متاحة افتراضيًا لجميع المستخدمين المسجّلين، وهو الوضع المناسب عادةً لطلبات الإجازة. أما في حال وجود خدمة ينبغي ألا يستخدمها إلا فريق الموارد البشرية، مثل **تعديل الراتب**، فاتّبع الخطوات الآتية:

1. في **أذونات وصول المجموعة** لمجموعة **الموارد البشرية**، اختر **إضافة إذن**.
2. في **الكائن**، اختر الخدمة، ثم اختر **جمهور الخدمة**، واحفظ.

تقصر إضافة مجموعة إلى جمهور الخدمة إتاحة هذه الخدمة على الأشخاص والمجموعات المدرَجين في قائمة جمهورها، فلا يراها بقية الموظفين في **دليل الخدمات** بعد ذلك. وإذا كانت الخدمة متاحة أيضًا للزوّار الذين لم يسجّلوا الدخول، فاطلب من بانيها تغيير ذلك أولًا؛ إذ لا يمكن أن تكون الخدمة متاحة للزوّار ومقصورة على قائمة محددة في آن واحد.

الخطوة 4: وجّه العمل إلى الموارد البشرية (إعداد يضبطه باني الخدمة)

تتيح المراقبة الاطّلاع فقط؛ فإذا كان على الموارد البشرية أيضًا أن تتّخذ إجراءً في الطلبات – كالموافقة أو الرفض أو الإعادة للتعديل – فيجب أن تملك مجموعة الموارد البشرية خطوات سير العمل المعنيّة، فتصل الطلبات حينئذ إلى **الوارد** لدى أعضاء الفريق. ونظرًا لأن ملكية الخطوات تُحدَّد ضمن تصميم الخدمة، اطلب من باني الخدمة أن يجعل مجموعة **الموارد البشرية** (أو دور **مدير الموارد البشرية**) مالكةً لتلك الخطوات.

تحقّق من النتيجة

1. افتح **الإدارة › إدارة الوصول › أذونات وصول الكائن**، واختر إحدى خدمات الموارد البشرية؛ ستجد مجموعة الموارد البشرية مدرَجة وموسومة بـ**المتابِعين**.
2. اطلب من أحد أعضاء الموارد البشرية فتح **المتابعة**؛ سيرى طلبات خدمات الموارد البشرية ولا شيء غيرها.
3. اطلب من شخص من خارج الموارد البشرية فتح **المتابعة**؛ فلن تظهر له طلبات الموارد البشرية.

استكشاف الأخطاء وإصلاحها

لا ترى الموارد البشرية الطلبات في «المتابعة». تحقّق من إدراج المجموعة ضمن مراقبي تلك الخدمة تحديدًا (الخطوة 1)، ومن أن الشخص عضو في مجموعة الموارد البشرية، ثم اطلب منه تحديث الصفحة.

ترى الموارد البشرية طلبات قسم آخر. قد تكون مجموعة الموارد البشرية مدرَجة ضمن مراقبي تلك الخدمة، أو تملك خطوة في سير عملها. راجع **أذونات وصول المجموعة** لمجموعة الموارد البشرية، واسأل باني الخدمة الأخرى عن مالكي خطواتها. وتحقّق كذلك من أذونات وصول الشخص نفسه في **أذونات وصول المستخدم**، فقد يكون قد حصل عليها عبر مجموعة أو دور آخر.

يرى أحد أعضاء الموارد البشرية كل الطلبات في الإدارة. لديه **تعديل** أو **إدارة** على مستوى النظام، أو **تعديل** على الوحدة التي تضمّ الخدمات. اخفض مستواه في **أذونات المدير**، أو في تبويب **الأذونات** الخاص بالوحدة.

للتعمّق أكثر

لبُناة التطبيقات: تجد حقل **المراقبون** وإعدادات الظهور ضمن تصميم الخدمة أيضًا، ويشرح سير العمل – إسناد المالك [بناء التطبيقات › سير العمل والاعتمادات] مالكي الخطوات · ما يراه المستخدمون النهائيون: الخدمات والطلبات [استخدام أسس › الخدمات وتقديم الطلبات] · لمطوّري التكامل: واجهة برمجة الأذونات – طلبات الخدمات [التكامل والتوسعة › واجهة الأذونات البرمجية]

أنشئ رمز API لعملية تكامل

هذا الدليل الإجرائي موجّه إلى مسؤولي القاطن. عندما يحتاج نظام آخر – أداة رواتب، أو برنامج نصي للتقارير، أو منصة أتمتة – إلى قراءة بياناتك في أسس أو الكتابة فيها، تمنحه **رمز API**. وستتعلّم هنا كيف تنشئ الرمز، وتمنحه الوصول الذي تحتاج إليه عملية التكامل تحديدًا، وتسلّمه إلى المطوّر بأمان، ثم تستبدله أو تلغيه لاحقًا.

كيف تعمل رموز API

يرتبط رمز API بـ**مستخدم تطبيق**: أي مُدخل مستخدم يمثّل نظامًا لا شخصًا. ولا يستطيع مستخدم التطبيق تسجيل الدخول إلى البوابة. أما النظام الذي يحمل رمزه فيتصرّف بصفة ذلك المستخدم، فلا يستطيع تنفيذ أي إجراء إلا في حدود ما تسمح لمستخدم التطبيق بفعله.

ولا يُنشأ الرمز وحده أبدًا؛ بل تضيف مستخدم تطبيق، فتنشئ المنصة الرمز له و**ترسله إليك بالبريد الإلكتروني**، بصفتك من أضاف المستخدم. ولا يُعرض الرمز على الشاشة، ولا يستطيع أحد قراءته مجددًا في وقت لاحق. فإن ضاع، فأعِد إنشاءه.

مثال: تحتاج أداة التقارير لدى فريق المالية إلى قراءة طلبات الشراء المعتمدة. فتضيف مستخدم تطبيق باسم **تقارير المالية**، وتشارك معه معرضًا لطلبات الشراء يُظهر ما تحتاج إليه الأداة دون غيره، وترسل رمزه إلى المطوّر الذي يُعِدّ الربط. وتقرأ الأداة البيانات عبر ذلك المعرض.

قبل أن تبدأ

- تحتاج إلى إذن إضافة المستخدمين في **الإدارة › المنظمة › المستخدمون**. ولإعادة إنشاء رمز لاحقًا، تحتاج إلى مستوى **إدارة** على النظام.
- يجب أن يكون لحسابك أنت عنوان بريد إلكتروني صالح، إذ يُرسل الرمز الجديد إليك بالبريد.
- اتفق مع المطوّر على البيانات التي ستقرؤها عملية التكامل أو تغيّرها. وخصّص لكل عملية تكامل مستخدم تطبيق مستقلًا، لتتمكن من إبطال أحدها دون تعطيل البقية.

الخطوة 1: إضافة مستخدم التطبيق

1. افتح **الإدارة › المنظمة › المستخدمون**، ثم اختر **إضافة مستخدم**.
2. في **المعلومات الاساسية**، أدخل اسمًا يوضّح الغرض من عملية التكامل، مثل **تقارير المالية**.
3. اضبط **نوع المستخدم** على **تطبيق**.
4. املأ **معلومات الحساب** وفق متطلبات مؤسستك.
5. في **معلومات التطبيق**:
   - في **الاسم**، أدخل اسم التطبيق.
   - حدّد مدة صلاحية الرمز. فعّل **غير منته** لإنشاء رمز لا تنتهي صلاحيته أبدًا، أو اتركه معطّلًا واضبط **تاريخ الانتهاء**. ويتوقف الرمز عن العمل في نهاية ذلك اليوم.
6. اختر **حفظ**.

ستتلقى خلال وقت قصير رسالة بريد إلكتروني تتضمن رمز API الجديد. وقد تكون مؤسستك قد غيّرت أسماء بعض هذه الحقول، لكن الإعداد الحاسم هو نوع المستخدم.

> ⚠ **تعامل مع الرمز كما تتعامل مع كلمة المرور**
>
> يستطيع كل من يحمل الرمز أن يتصرّف بصفة مستخدم التطبيق هذا. فلا تلصقه في المحادثات أو التذاكر أو المستندات المشتركة، بل سلّمه إلى المطوّر عبر مدير كلمات المرور أو مخزن الأسرار المعتمد في مؤسستك، ثم احذف رسالة البريد.

الخطوة 2: منح مستخدم التطبيق الوصول الذي يحتاج إليه فقط

لا يستطيع مستخدم التطبيق الجديد فعل شيء يُذكر حتى تمنحه الوصول، فامنحه إياه بالطريقة نفسها التي تمنحه بها لمستخدم يمثّل شخصًا:

1. امنحه مستوى صلاحية على النظام، ويكون عادةً **مقيّد**. راجع امنح الجميع مستوى أساسيًا.
2. امنحه الوصول إلى البيانات التي تتعامل معها عملية التكامل. فلكي **يقرأ** المُدخلات، شارك معه معرضًا للكيان – مثل معرض لطلبات الشراء – ويقرأ المطوّر البيانات عبر ذلك المعرض. راجع امنح مجموعة وصولًا إلى معرض أو صفحة أو تقرير أو خدمة؛ ولمستخدم واحد، أضِف الإذن من **أذونات وصول المستخدم** بدلًا من ذلك. ولكي يكتب المُدخلات، أو يقرأها من الكيان مباشرةً، امنحه **تعديل** على الكيان. راجع الأذونات والوصول.

لا يكفي مستوى «عرض» على الكيان لقراءة مُدخلاته. فمستوى «عرض» يُظهر تصميم الكيان لا مُدخلاته، ولذلك حين تطلب عملية التكامل مُدخلات الكيان منه مباشرةً تتلقّى قائمة فارغة، دون أي خطأ. وإذا كانت عملية التكامل تقتصر على القراءة، ففضّل مشاركة معرض على منح **تعديل**، لأن «تعديل» يتيح لها تغيير المُدخلات أيضًا. ولا تمنح مستخدم التطبيق مستوى **تعديل** أو **إدارة** على النظام ما لم تكن عملية التكامل تدير المنصة فعلًا.

الخطوة 3: تسليم الرمز إلى المطوّر

أرسل إلى المطوّر:

- الرمز، عبر قناة آمنة؛
- عنوان أسس الخاص بمؤسستك (العنوان الذي يستخدمه المستخدمون لتسجيل الدخول)؛
- البيانات التي يستطيع مستخدم التطبيق الوصول إليها.

أما التعليمات الموجّهة إلى المطوّر – أي كيفية إرسال الرمز مع كل طلب – فتجدها في استخدام رمز API [التكامل والتوسعة › استخدم رمز API].

استبدال الرمز (إعادة الإنشاء)

أعِد إنشاء الرمز عند الاشتباه في تسرّبه، أو إذا فقده المطوّر، أو وفق جدول تدوير الرموز المعتمد في مؤسستك. ويظل مستخدم التطبيق وأذونات وصوله وسجلّه كما هي.

1. افتح **الإدارة › المنظمة › المستخدمون** وابحث عن مستخدم التطبيق.
2. افتح قائمته، ثم اختر **إعادة إنشاء الرمز**. (يتوفر هذا الخيار أيضًا في القائمة أعلى صفحة مستخدم التطبيق نفسه.)
3. اختر **إعادة إنشاء** للتأكيد.

يُرسل الرمز الجديد بالبريد الإلكتروني **إليك** أنت، بصفتك المسؤول الذي أعاد إنشاءه – وليس إلى من أنشأ مستخدم التطبيق. ويستمر الرمز القديم في العمل خلال مدة سماح (24 ساعة ما لم يغيّرها المشغّل)، لإتاحة الوقت للمطوّر للانتقال إلى الرمز الجديد.

لا يمكنك إعادة إنشاء رمز مستخدم تطبيق مؤرشف. فاستعِده أولًا، أو أضِف مستخدم تطبيق جديدًا.

إبطال الرمز

- **لإيقاف عملية تكامل مؤقتًا**، افتح مستخدم التطبيق واختر **تعطيل الحساب**، فيتوقف رمزه عن العمل. واختر **تفعيل الحساب** للسماح باستخدامه مجددًا.
- **لإنهاء عملية تكامل نهائيًا**، أرشِف مستخدم التطبيق، فيتوقف رمزه عن العمل ولا يمكن إعادة إنشائه.

وفي الحالتين، قد يستغرق الأمر نحو خمس دقائق حتى يُرفض الرمز في كل مكان.

معلومات مفيدة

- **لا يُرسل الرمز إلا بالبريد الإلكتروني.** فعند الإنشاء يُرسل إلى من أضاف مستخدم التطبيق، وعند إعادة الإنشاء يُرسل إلى المسؤول الذي أعاد إنشاءه. وإذا تعذّر على المنصة العثور على حساب من أضاف مستخدم التطبيق، فلا يُنشأ أي رمز – أعِد إنشاءه من قائمة المستخدم.
- **تاريخ الانتهاء مُلزِم.** فبعد **تاريخ الانتهاء** يتوقف الرمز عن العمل وتُرفض عملية التكامل. ولا تغيّر إعادةُ الإنشاء تاريخَ الانتهاء؛ لذا عدّل مستخدم التطبيق لتمديده.
- **التطبيقات المثبّتة من المتجر والوظائف التي تعمل على الخادم** تحصل تلقائيًا على مستخدمي تطبيقات خاصين بها. فلا تنشئ رموزًا لها. وعند إعادة إنشاء رمز الوظيفة، لا يُرسل بالبريد الإلكتروني، بل يُمرَّر مباشرةً إلى الوظيفة.

استكشاف الأخطاء وإصلاحها

لم تصلني رسالة البريد التي تحمل الرمز. تحقق من مجلد الرسائل غير المرغوب فيها، ومن أن عنوان البريد الإلكتروني في حسابك أنت صحيح. وإذا ضاعت الرسالة، فأعِد إنشاء الرمز.

تُرفض عملية التكامل بعد أن كانت تعمل. تحقق من أن مستخدم التطبيق ليس معطّلًا أو مؤرشفًا، ومن أن **تاريخ الانتهاء** الخاص به لم يمضِ. وإذا كنت قد أعدت إنشاء الرمز مؤخرًا، فقد توقف الرمز القديم عن العمل عند انتهاء مدة السماح.

تتلقّى عملية التكامل قائمة فارغة، دون أي خطأ. لا يستطيع مستخدم التطبيق سرد مُدخلات ذلك الكيان. ولا يكفي مستوى «عرض» على الكيان: شارك معرضًا مع مستخدم التطبيق واقرأ البيانات عبره، أو امنحه **تعديل** على الكيان.

تُرفض عملية التكامل لنوع واحد فقط من المُدخلات. لا يملك مستخدم التطبيق إذن الوصول إلى تلك البيانات. تحقق من ذلك في **الإدارة › إدارة الوصول › أذونات وصول المستخدم**.

للتعمّق أكثر

لمطوّري التكامل: استخدام رمز API [التكامل والتوسعة › استخدم رمز API] · اختيار بيانات الاعتماد [التكامل والتوسعة] · دورة حياة الرموز [التكامل والتوسعة]

فيديو: إدارة الأذونات (بما فيها الحقول الحساسة)

فيديو قصير (نحو دقيقتين) لمسؤولي القاطن: امنح مجموعةً إذن الوصول إلى كيان، وتعرّف إلى سبب اشتراط مستوى **تعديل** للوصول إلى المُدخلات، ثم احمِ حقلًا حساسًا مثل *الراتب* كي لا يقرأه إلا من تختارهم.

> **التسجيل غير متاح بعد**
>
> إلى أن يُنشر الفيديو، اتّبع الخطوات المكتوبة في إدارة الأذونات والأذونات الحساسة.

اللوحة القصصية

هذا هو النص الذي سيُعتمد في التسجيل.

المشهد	الإجراء على الشاشة	التعليق الصوتي (النص)	المدة
1. المقدمة	كيان **الموظفون** في الإدارة.	«سنحدّد من يستطيع رؤية مُدخلات الموظفين ومن يستطيع تغييرها، ثم نحمي حقل الراتب.»	8 ثوانٍ
2. فتح الأذونات	افتح تبويب **الأذونات** الخاص بالكيان.	«لكل وحدة ولكل كيان تبويب خاص بالأذونات.»	8 ثوانٍ
3. المستويات	اعرض المستويات: مقيّد، وعرض، ومطوّر، وتعديل، وإدارة.	«للوصول مستويات: مقيّد، وعرض، ومطوّر، وتعديل، وإدارة.»	12 ثانية
4. منح «عرض»	امنح مجموعة **الموارد البشرية** مستوى **عرض**.	«يتيح مستوى عرض لمجموعة الموارد البشرية الاطّلاع على تصميم الكيان وفتح المعارض المشارَكة معها.»	10 ثوانٍ
5. المُدخلات تتطلب «تعديل»	أشِر إلى أن مستوى «عرض» لا يُظهر المُدخلات في الإدارة.	«لاستعراض المُدخلات نفسها أو فتحها في الإدارة، يحتاج المستخدم إلى مستوى تعديل؛ أما معظم المستخدمين فيستخدمون المعارض المشارَكة بدلًا من ذلك.»	12 ثانية
6. منح «تعديل»	امنح مجموعة **مديرو الموارد البشرية** مستوى **تعديل**.	«يحصل مديرو الموارد البشرية على مستوى تعديل، فيستطيعون العمل على المُدخلات.»	8 ثوانٍ
7. الوصول يتراكم	اعرض شخصًا ينتمي إلى المجموعتين.	«تتراكم أذونات الوصول: فمن ينتمي إلى المجموعتين يحصل على المستوى الأعلى. ولسحب إذن الوصول، أزِل المنحة التي تمنحه.»	12 ثانية
8. مواضع أخرى	اعرض **الإدارة › إدارة الوصول**.	«يمكنك أيضًا إدارة أذونات الوصول لكل مستخدم، ولكل مجموعة، وللمعارض والصفحات والتقارير.»	12 ثانية
9. الحقل الحساس	في مصمّم الكيان، ضع علامة **حساس** على حقل **الراتب**.	«الآن نحمي الراتب، فنضع على الحقل علامة حساس.»	12 ثانية
10. الحجب	اعرض القيمة بالصيغة `****` مع أيقونة قفل.	«يرى الجميع الآن نجومًا، حتى المسؤولون، لأن المنصة نفسها تُخفي القيمة، وليس الشاشة وحدها.»	12 ثانية
11. منح الحقل	في **الأذونات الحساسة**، أضِف لمجموعة **مديرو الموارد البشرية** منحةً على حقل **الراتب**؛ واعرض أيقونة العين.	«نمنح مديري الموارد البشرية إذنًا حساسًا، فتظهر لهم أيقونة عين، ويستطيعون كشف القيمة بعد تأكيد هويتهم.»	12 ثانية
12. الخاتمة	تبويب الأذونات بعد ضبطه.	«هذا كل شيء: الأشخاص المناسبون يرون المُدخلات المناسبة، وتبقى الرواتب سرّية.»	8 ثوانٍ

أسئلة الإدارة الشائعة

إجابات موجزة عن أكثر الأسئلة التي يطرحها مسؤولو القاطن، مع رابط في كل إجابة إلى صفحة تشرح الخطوات. أما أسئلة الاستخدام اليومي لـ أسس فتجدها في أسئلة استخدام المنصة الشائعة [استخدام أسس › أسئلة مستخدمي البوابة].

الأشخاص والحسابات

هل يستطيع الأشخاص إنشاء حساباتهم بأنفسهم؟

لا، فالمدير هو من ينشئ كل حساب. وإذا كانت مؤسستك تستخدم الدخول الموحّد، فبإمكان مشغّل المنصة تهيئة النظام لإنشاء حسابات الأشخاص تلقائيًا عند أول تسجيل دخول لهم بحساب الشركة. راجع إدارة المستخدمين وطرق تسجيل الدخول والدخول الموحّد.

كيف يحصل المستخدم الجديد على كلمة مروره؟

عندما تنشئ الحساب، يتلقّى صاحبه رسالة بريد إلكتروني تتضمن رابطًا لتعيين كلمة مروره بنفسه. أما من يسجّلون الدخول بحساب الشركة (الدخول الموحّد) فلا يحتاجون إلى كلمة مرور.

هل أستطيع رؤية كلمة مرور شخص ما أو تعيينها؟

لا. كل ما تستطيعه هو أن ترسل إليه رسالة إعادة تعيين كلمة المرور، ليختار كلمة المرور الجديدة بنفسه. راجع إدارة المستخدمين.

قُفل حساب شخص بعد إدخال كلمة مرور خاطئة مرات كثيرة. كيف أفتحه؟

لا يوجد زر لفتح القفل؛ إذ يُرفع القفل تلقائيًا بعد مدة تطول كلما تكرر القفل. ولتمكين صاحب الحساب من الدخول فورًا، أرسل إليه رسالة إعادة تعيين كلمة المرور.

ما الفرق بين تعطيل المستخدم وأرشفته؟

التعطيل يوقف الحساب فورًا ويُخرج صاحبه من جميع جلسات تسجيل الدخول؛ وإذا أعدت تفعيله استطاع الدخول بكلمة مروره القديمة. أما **الأرشفة** فتحذف بيانات الدخول الخاصة بالحساب حذفًا تامًا، فإذا استعدت مستخدمًا مؤرشفًا وجب عليه تعيين كلمة مرور جديدة عبر الرسالة التي تصله بالبريد الإلكتروني. لذا، إذا كان الشخص المغادر قد يعود، فاختر التعطيل. راجع إدارة المستخدمين.

هل أستطيع استيراد مستخدمينا من Active Directory أو Microsoft Entra ID؟

نعم، لكن مشغّل المنصة هو من يجري الاستيراد؛ إذ لا توجد شاشة استيراد في **الإدارة**. حدّد له الأشخاص والمجموعات المطلوب استيرادها. راجع المستخدمون من دليل مؤسستك.

الوصول

ينتمي شخص إلى عدة مجموعات. أيّ وصول يحصل عليه؟

الأعلى: فالوصول الذي يأتيه من منحه الشخصية ومن مجموعاته وأدواره يتراكم، ولا شيء منها ينتقص منه. راجع كيف تتراكم المنح.

كيف أتحقق مما يستطيع شخص الوصول إليه؟

افتح **الإدارة › إدارة الوصول › أذونات وصول المستخدم** واختر الشخص. راجع تحقّق مما يستطيع شخص الوصول إليه.

كيف أسحب الوصول؟

أزِل المنحة التي تمنحه هذا الوصول، ثم راجع مجموعاته وأدواره؛ فإن ظل أحدها يمنحه الوصول، فسيحتفظ به. راجع تغيير الوصول أو إزالته.

يستطيع شخص فتح معرض، لكنه لا يرى المُدخلات في الإدارة. لماذا؟

تتطلب رؤية مُدخلات كيان ما في **الإدارة** صلاحية **تعديل** على ذلك الكيان أو على وحدته. ولا يحتاج معظم المستخدمين إلى ذلك، إذ يعملون من خلال المعارض والصفحات والخدمات التي تشاركها معهم. راجع الأذونات والوصول.

هل يرى مسؤول النظام الحقول الحساسة؟

لا، ما لم تكن لديه منحة. فلا أحد، حتى مسؤول النظام، يستطيع رؤية قيمة حساسة ما لم يكن لديه إذن حساس يتيح ذلك، وحتى عندئذ عليه بدء جلسة كشف. راجع الأذونات الحساسة.

كيف أجد كل من يستطيع رؤية حقل حساس بعينه؟

راجع قائمة المنح الخاصة بالحقل نفسه **ومعها** مربع الحوار **الأذونات الموروثة** الخاص به؛ فلا تظهر القائمة الكاملة إلا بمراجعتهما معًا. راجع الأذونات الموروثة.

هل يمكن منح الوصول لمدة محدودة؟

نعم، في الحقول الحساسة: حدّد **مدة الصلاحية** للمنحة، فتنتهي صلاحيتها تلقائيًا. راجع المنح التي تنتهي صلاحيتها.

التفويض

كيف أتيح لشخص أن ينوب عن زميل غائب؟

أنشئ تفويضًا من الزميل إلى من ينوب عنه، وحدّد فيه تاريخ البدء وتاريخ الانتهاء وما يشمله. راجع التفويض.

هل يمكن أن يتلقى النائب إشعارات زميله ورسائل بريده الإلكتروني؟

نعم، إذا فعّلت **حول الإشعارات** و**حول البريد الالكتروني** في التفويض، ويستمر الزميل في تلقّي كل شيء. `Since 1.10` راجع نسخ للمفوَّض إليه.

كيف أنهي تفويضًا ليس له تاريخ انتهاء؟

اجعله غير نشط، أو حدّد له تاريخ انتهاء، أو أرشفه.

المساحات والمنظمة

ما الفرق بين المساحة والنطاق؟

المساحة منطقة عمل مستقلة لها بياناتها وأعضاؤها، أما **النطاق** فهو عنوان ويب يستخدمه الأشخاص، وله خيارات تسجيل الدخول الخاصة به. راجع المساحات والنطاقات.

أضفت شخصًا إلى مساحة لكنه لا يراها. لماذا؟

تأكد من أنه مُدرج في تبويب **المستخدمين** في المساحة، وأن المساحة نشطة، ثم اطلب منه إعادة تحميل الصفحة أو تسجيل الدخول من جديد. راجع المساحات والنطاقات.

ما الفرق بين إلغاء تفعيل المساحة وتعطيل واجهات المستخدم النهائي فيها؟

إلغاء تفعيل المساحة يوقف المساحة كلها عن العمل، أما **تعطيل واجهات المستخدم النهائي** فيمنع المستخدمين من استخدام تطبيقاتها، بينما يمكنك مواصلة العمل عليها في الإدارة. راجع ضع المساحة في وضع الصيانة أو أوقفها عن العمل.

أين أغيّر اللغة والمنطقة الزمنية وتنسيق التاريخ؟

في مُدخل إعدادات ضمن **الإدارة › الواجهات › الإعدادات**: مُدخل واحد للمنظمة كلها، ومُدخلات اختيارية لمساحة أو لشخص. راجع إعدادات المنظمة.

هل أستطيع تغيير اسم منتجنا أو شعارنا؟

ليس من **الإدارة**. فهما يأتيان من النشر لديكم أو من العلامة التجارية لمؤسستك؛ اسأل مشغّل المنصة. أما السمات والخطوط الخاصة بمؤسستك فبإمكانك إضافتها بنفسك. راجع إعدادات المنظمة والمظهر.

هل أستطيع تعديل قائمة العملات؟

لا، فقائمة العملات واحدة للجميع.

كيف أحدد ساعات العمل والعطلات؟

راجع ساعات العمل ومراقبة الوقت.

تسجيل الدخول

هل يستطيع الأشخاص تسجيل الدخول بحساب Microsoft أو بحساب شركة آخر؟

نعم. تنسّق إعداد ذلك مع الجهة التي تدير مزوّد الهوية في شركتك، ثم يتولى مشغّل المنصة ربطه. راجع طرق تسجيل الدخول والدخول الموحّد.

فجأة لم يعد أحد يستطيع تسجيل الدخول. ماذا أفعل؟

اطلب من مشغّل المنصة التحقق أولًا من خدمة التحقق البشري؛ فإذا توقفت، توقف تسجيل الدخول للجميع. راجع التحقق البشري.

لماذا صار كل من لديه رقم هاتف يُطلب منه رمز دخول؟

لأن رموز الدخول عبر واتساب أصبحت مهيّأة؛ وعند تهيئتها، يُطلب الرمز من كل من لديه رقم هاتف موثّق. `Since 1.10` راجع رموز واتساب.

الرسائل والمراقبة

يقول شخص إنه لم يتلقَّ رسالة بريد إلكتروني. كيف أتحقق؟

افتح **الإدارة › المراقبة › السجلات**، ثم تبويب **البريد الإلكتروني**، وتحقق من **الحالة** الخاصة بالرسالة. فإن لم تجد أثرًا للرسالة، فتحقق من التفاعل في **سجل التفاعلات**. راجع المراقبة: السجلات والتدقيق.

لا أحد يتلقى الرسائل النصية. لماذا؟

تحتاج الرسائل النصية إلى مزوّد خدمة SMS يتولى مشغّل المنصة ربطه؛ فاسأله إن كان قد هيّأه.

تظهر رسائل واتساب لدينا بالحالة «لم تُرسل (الإرسال معطل)». لماذا؟

الإرسال الفعلي عبر واتساب متوقف في النشر لديكم، ومشغّل المنصة هو من يفعّله. `Since 1.10`

هل يستطيع المديرون قراءة روابط إعادة تعيين كلمة المرور أو رموز API في سجل البريد؟

لا، إذ تُحذف من النسخة المحفوظة في السجل. راجع الإشعارات وقوالب البريد الإلكتروني.

كيف أعرف من غيّر مُدخلًا أو معرضًا أو إذنًا؟

افتح **الإدارة › المراقبة › سجل التدقيق**، ورشّح النتائج حسب **اسم الحدث** والتاريخ. راجع اعرف من غيّر ماذا.

هل جرى تشغيل تفاعل ما، وماذا فعل؟

افتح **الإدارة › المراقبة › سجل التفاعلات**، ورشّح النتائج حسب التفاعل. أما التفاعل الذي لم يتحقق شرط مرشّحه فلا يُسجَّل له صف. `Since 1.10` راجع تحقق مما إذا كان التفاعل قد جرى تشغيله.

الرخصة

قائمة الإدارة غائبة عند الجميع. لماذا؟

الأرجح أن رخصتك لا تشمل الإدارة؛ فاطلب من المورّد إضافتها. راجع رخصتك.

تصلنا تحذيرات بشأن حد المُدخلات. فما العمل؟

أرشف المُدخلات التي لم تعد تعمل عليها – فيُحتسب كل منها عندئذ بربع مُدخل – أو احذفها، واطلب من المورّد رفع الحد. وعند بلوغ 110% من الحد تُرفض المُدخلات الجديدة، ولا توجد في الإصدار 1.10 شاشة لعرض الاستهلاك. `Since 1.10` راجع حدود الخطة.

> **للتعمّق أكثر**
>
> للمشغّلين ومطوّري التكامل: الإدارة: أسئلة تقنية