



عرض المنتج · الإصدار 1.1

حوكمة AD وإعادة اعتماد الصلاحيات

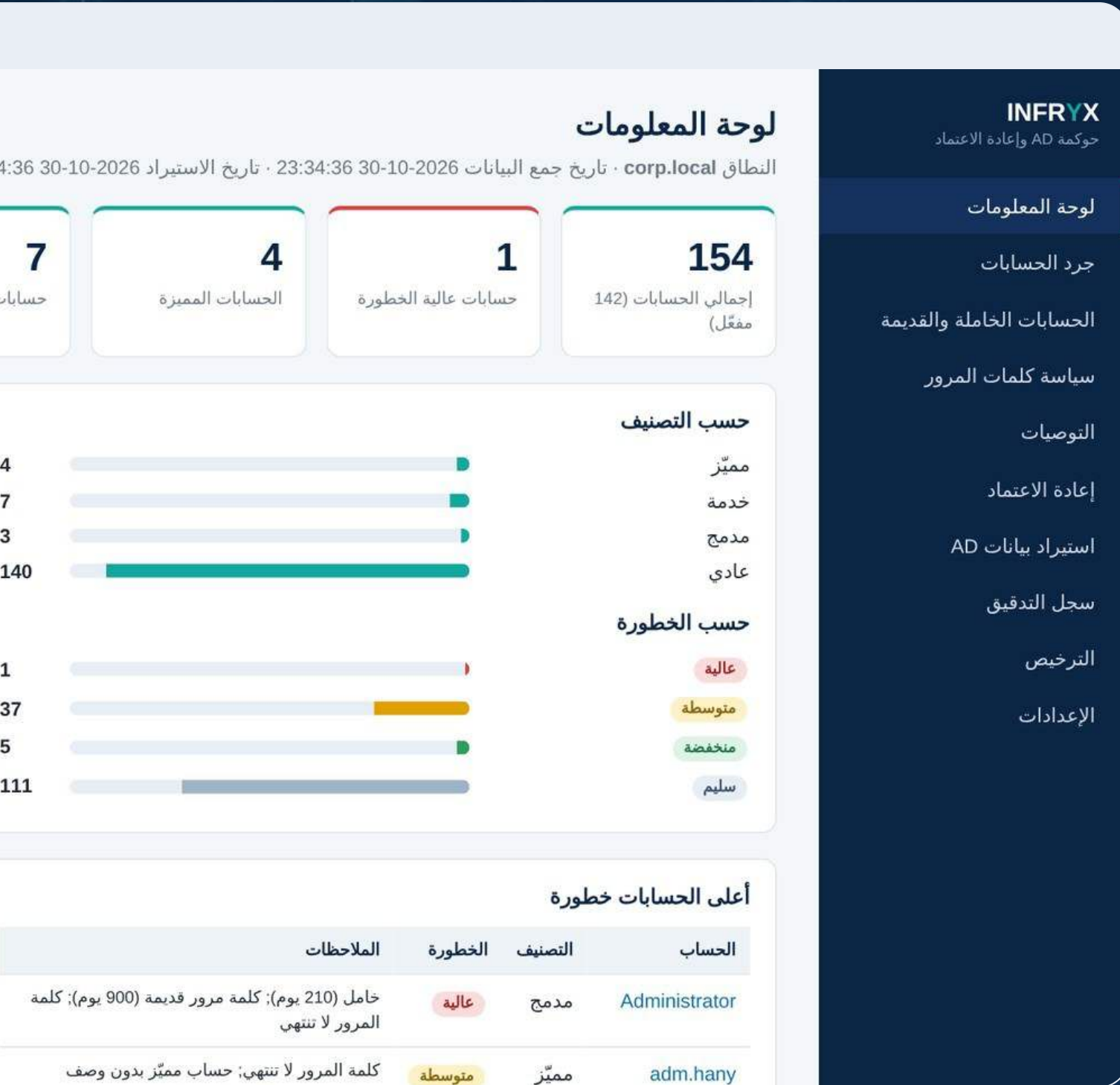
اعرف من يملك صلاحيات في Active Directory الخاص بك، وأثبت ذلك للمراجعين.

إعادة اعتماد الصلاحيات

تحليل المخاطر

جرد الحسابات

أدلة جاهزة للتدقيق



لماذا تحتاج صلاحيات Active Directory إلى حوكمة؟



أدلة تُجمع يدويًا

جداول تُجهَّز على عجل قبل كل عملية تدقيق.



كلمات مرور ضعيفة

كلمات مرور لا تنتهي وسياسات أقل من المستوى الموصى به.



بلا مالك ولا غرض

حسابات خدمة ومشاركة لا يستطيع أحد تبريرها أمام المراجع.



حسابات منسية

حسابات خاملة أو لم تُستخدم قط تبقى مفعلة لسنوات.



صلاحيات مميزة مخفية

صلاحيات إدارية داخل مجموعات متداخلة لا يراجعها أحد.

مسار واحد من بيانات AD الخام إلى أدلة التدقيق



كيف يعمل النظام



✓ لا يخزن التطبيق أي بيانات اعتماد

✓ لا يحتاج اتصالاً بالإنترنت للترخيص

✓ داخل شبكتك: بياناتك تبقى على خادمك

حالة الدليل في نظرة واحدة

مؤشرات رئيسية

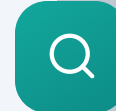
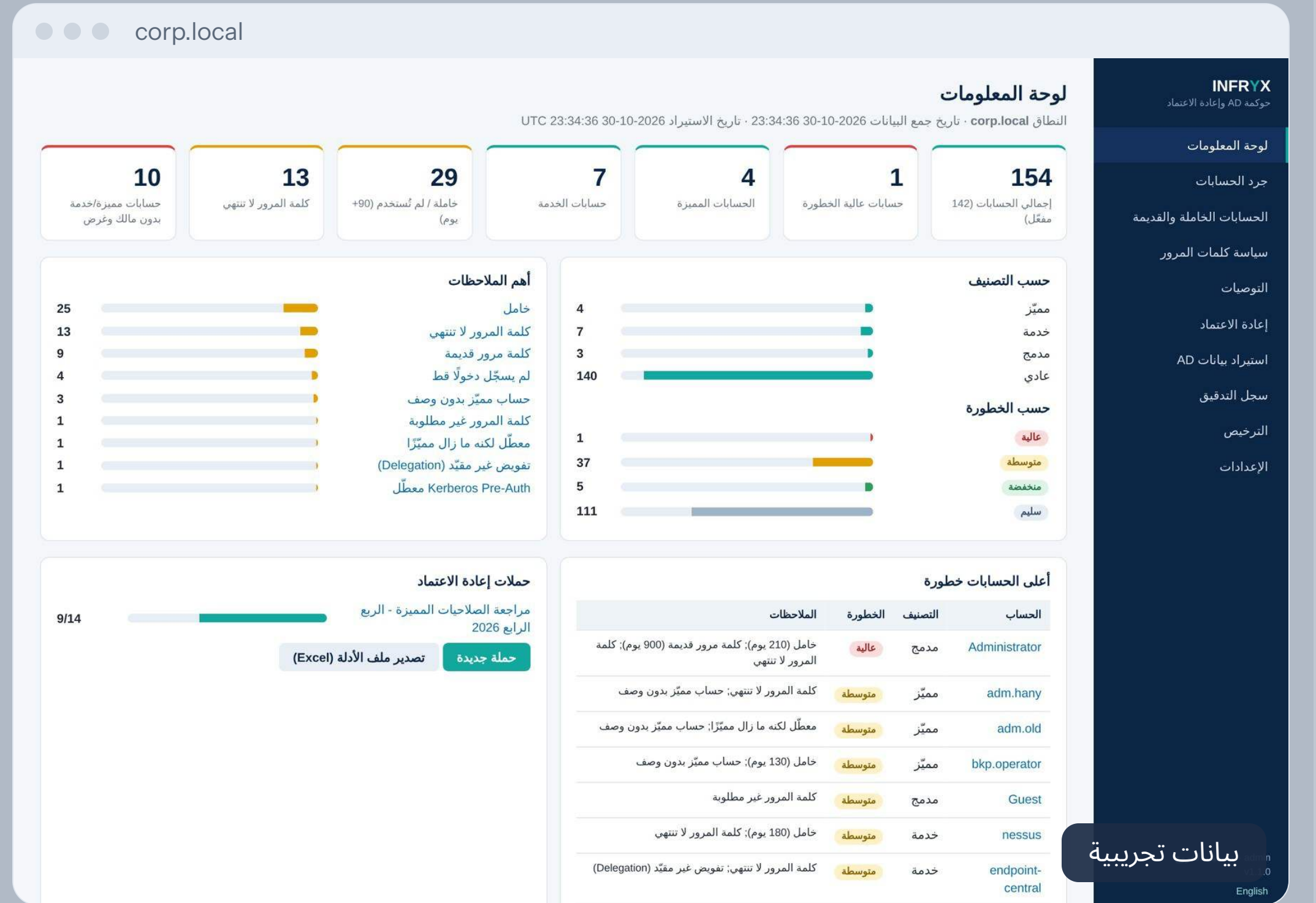
إجمالي الحسابات والعالية الخطورة والمميزة وحسابات الخدمة والخاملة وغير المؤثقة.

التوزيع

حسب التصنيف وحسب مستوى الخطورة.

إلى التفاصيل مباشرة

أهم الملاحظات وأعلى الحسابات خطورة، وبضغطة واحدة تصل إلى سجل الحساب.



جرد الحسابات مع تصنيف تلقائي

مميّز
عضو (بشكل متداخل) في مجموعة AD
AdminCount = 1 أو عالية الصلاحيات،

خدمة
لديه SPN أو اسم بنمط حسابات الخدمة

مدمج
Administrator و krbtgt و Guest وما
شابهها من الحسابات الافتراضية

عادي
بقية الحسابات

عالية • متوسطة • منخفضة • سليم

تُحسب الخطورة من الملاحظات المكتشفة على كل حساب.

المالك والغرض

تعيين جماعي، وكل تغيير في التصنيف يُسجّل في سجل التدقيق.

corp.local

البحث

التصنيف الكل

الحالة الكل

الخطورة الكل

المالك والغرض الكل

إعادة ضبط

الاسم أو القسم أ

الحساب أو الاسم أو القسم أ

مالك العمل (المسؤول)

بريد المالك

الغرض من الحساب

تغيير التصنيف

مثال: مدير الحسابات

لماذا يوجد هذا الحساب؟

(بدون تغيير)

تطبيق على المحدد

الحساب	التصنيف	الحالة	آخر دخول	المالك	الغرض	الخطورة	الملاحظات
Administrator Administrator	مدمج	خامل	2026-04-03 210 يوم مضى	—	—	عالية	خامل (210 يوم): كلمة مرور قديمة (900 يوم): كلمة المرور لا تنتهي
adm.hany Hany Adel (Admin)	مميّز	نشط	2026-10-12 18 يوم مضى	—	—	متوسطة	كلمة المرور لا تنتهي: حساب مميّز بدون وصف
adm.old Old Admin	مميّز	معطل	2025-09-25 400 يوم مضى	—	—	متوسطة	معطل لكنه ما زال مميّزًا: حساب مميّز بدون وصف
bkp.operator Backup Operator	مميّز	خامل	2026-06-22 130 يوم مضى	—	—	متوسطة	خامل (130 يوم): حساب مميّز بدون وصف
endpoint-central Endpoint Central	خدمة	نشط	2026-10-23 7 يوم مضى	—	—	متوسطة	كلمة المرور لا تنتهي: تفويض غير مقيّد (Delegation)
Guest Guest	مدمج	معطل	—	—	—	متوسطة	كلمة المرور غير مطلوبة
nessus Nessus Scanner	خدمة	خامل	2026-05-03 180 يوم مضى	—	—	متوسطة	خامل (180 يوم): كلمة المرور لا تنتهي
svc_kerb Kerberoast legacy	خدمة	نشط	2026-10-12 18 يوم مضى	—	—	متوسطة	Metasploit Kerberos Pre-Auth معطل
a.farouk92 Ahmed Farouk 92	عادي	خامل	2026-06-07 145 يوم مضى	—	—	متوسطة	خامل (145 يوم)
a.hassan13 Amr Hassan 13	عادي	نشط	2026-10-23 7 يوم مضى	—	—	متوسطة	كلمة مرور قديمة (664 يوم): كلمة المرور لا تنتهي

INFRYX

حوكمة AD وإعادة الاعتماد

لوحة المعلومات

جرد الحسابات

الحسابات الخاملة والقديمة

سياسة كلمات المرور

التوصيات

إعادة الاعتماد

استيراد بيانات AD

سجل التدقيق

الترخيص

الإعدادات

admin
v1.1.0
English

بيانات تجريبية

الحسابات الخاملة وسلامة كلمات المرور

corp.local

INFRYX

حزمة AD وإعادة الاعتماد

لوحة المعلومات

جرد الحسابات

الحسابات الخاملة والقديمة

سياسة كلمات المرور

التوصيات

إعادة الاعتماد

استيراد بيانات AD

سجل التدقيق

الترخيص

الإعدادات

تقرير سياسة كلمات المرور

مقارنة سياسة الدومين الافتراضية والسياسات الدقيقة (Fine-Grained) بالمعايير المرجعية الشائعة (NIST SP 800-63B / CIS).

الإعداد	الحالي	الموصى به	النتيجة
الحد الأدنى لطول كلمة المرور	7	12 حرفًا أو أكثر (NIST/CIS: 14) للحسابات المميزة)	يحتاج مراجعة
سجل كلمات المرور	24	تذكر آخر 24 كلمة مرور	مطابق
تفعيل التعقيد (Complexity)	True	مفعل	مطابق
تشغيل قابل للعكس	False	معطل	مطابق
حد القفل (محاولات فاشلة)	5	بين 1 و10 محاولات فاشلة	مطابق
مدة القفل (دقيقة)	30	15 دقيقة أو أكثر	مطابق

أقصى عمر لكلمة المرور: 90 يوم - أدنى عمر: 1 يوم - نافذة القفل: 30 دقيقة.

السياسات الدقيقة (PSO)

الاسم	الأولوية	أدنى طول	السجل	أقصى عمر	التعقيد	القفل	تنطبق على
PSO-Admins	10	14	24	60d	True	3	Domain Admins

حسابات بها استثناءات في كلمة المرور

13

Administrator, adm.hany, svc_sql, svc_backup, ADSync

1

Guest

0

1

svc_kerb

9

Administrator, svc_sql, svc_backup, a.hassan13, h.fathy31

كلمة المرور لا تنتهي

كلمة المرور غير مطلوبة

تشغيل قابل للعكس

Kerberos Pre-authentication معطل

كلمة المرور قديمة

تصدير ملف الأدلة (Excel)

corp.local

INFRYX

حزمة AD وإعادة الاعتماد

لوحة المعلومات

جرد الحسابات

الحسابات الخاملة والقديمة

سياسة كلمات المرور

التوصيات

إعادة الاعتماد

استيراد بيانات AD

سجل التدقيق

الترخيص

الإعدادات

الحسابات الخاملة والقديمة

حسابات مفعلة لم تسجل دخولاً منذ 90 يومًا أو أكثر، أو لم تُستخدم قط، أو كلمة مرورها أقدم من 365 يومًا. الحدود قابلة للتعديل من الإعدادات. تم العثور على 37 حساب.

الحساب	التصنيف	آخر دخول	عمر كلمة المرور	المالك	الخطورة	الملاحظات
o.gamal1 Omar Gamal 1	عادي	لم يُستخدم	33 يوم	—	منخفضة	لم يسجل دخولاً قط
h.farouk14 Heba Farouk 14	عادي	لم يُستخدم	80 يوم	—	منخفضة	لم يسجل دخولاً قط
n.fathy114 Nour Fathy 114	عادي	لم يُستخدم	21 يوم	—	منخفضة	لم يسجل دخولاً قط
s.farouk124 Sara Farouk 124	عادي	لم يُستخدم	10 يوم	—	منخفضة	لم يسجل دخولاً قط
r.gamal86 Rania Gamal 86	عادي	2025-09-10 (415d)	41 يوم	—	متوسطة	خامل (415 يوم)
o.samir137 Omar Samir 137	عادي	2025-09-25 (400d)	63 يوم	—	متوسطة	خامل (400 يوم)
a.nabil69 Ahmed Nabil 69	عادي	2025-11-11 (353d)	34 يوم	—	متوسطة	خامل (353 يوم)
m.zaki3 Mona Zaki 3	عادي	2025-11-15 (349d)	64 يوم	—	متوسطة	خامل (349 يوم)
h.said112 Hany Said 112	عادي	2025-11-15 (349d)	38 يوم	—	متوسطة	خامل (349 يوم)

إعادة اعتماد

تصدير ملف الأدلة (Excel)

بيانات تجريبية

in .0 ish

الحسابات الخاملة والقديمة

حسابات مفعلة لم تسجل دخولاً منذ 90 يومًا أو أكثر (قابلة للتعديل)، أو لم تُستخدم قط، أو كلمة مرورها قديمة.

تقرير سياسة كلمات المرور

مقارنة سياسة الدومين والسياسات الدقيقة بمعايير مرجعية مثل NIST SP 800-63B و CIS.

7 / 17

INFRYX
AD-GOV

INFRYX AD-GOV · v1.1

حملات إعادة الاعتماد

1 تحديد النطاق ← 2 مراجعة كل حساب ← 3 تسجيل القرار ← 4 إغلاق الحملة وقفلها

أربعة قرارات

إبقاء · تعديل الصلاحيات · تعطيل · حذف

أدلة متسقة

تُثبت نسخة لحظية من الحسابات المحددة داخل الحملة.

مساءلة واضحة

المراجع والتاريخ وتعليق لكل قرار غير الإبقاء.

معالجة آمنة

يُولد سكريبت PowerShell بوضع WhatIf افتراضيًا.

corp.local

الحملة

مراجعة الصلاحيات المميزة - الربع الرابع 2026

الاستحقاق 15-12-2026 · النطاق: ممّيز، خدمة، مدمج · تمت مراجعة 9 من 14

إبقاء: 4

تعديل الصلاحيات: 2

تعطيل: 3

حذف: 0

قيد المراجعة: 5

الكل

تصدير ورقة الأدلة (Excel)

سكربت المعالجة (PowerShell - بوضع افتراضيًا)

إغلاق حتى مع وجود عناصر معلقة

إغلاق الحملة

القرار للعناصر المحددة

المراجع

تعليق (الرامي عدا قرار الإبقاء)

إبقاء

اسم المالك / المدير

تطبيق

الحساب	التصنيف	الخطورة	المالك / الغرض	الملاحظات وقت المراجعة	القرار
Administrator Administrator	مدمج	عالية	Domain Admins, Enterprise Admins, Schema Admins, Administrators	خامل (210 يوم); كلمة مرور قديمة (900 يوم); كلمة المرور لا تنتهي	قيد المراجعة
Guest Guest	مدمج	متوسطة		كلمة المرور غير مطلوبة	قيد المراجعة
endpoint-central Endpoint Central	خدمة	متوسطة		كلمة المرور لا تنتهي; تفويض غير مقيّد (Delegation)	قيد المراجعة
svc_kerb Kerberoast legacy	خدمة	متوسطة		Kerberos Pre-Auth معطل	قيد المراجعة
krbtgt krbtgt	مدمج	سليم			قيد المراجعة
adm.hany Hany Adel (Admin)	ممّيز	متوسطة	Domain Admins	كلمة المرور لا تنتهي; حساب ممّيز بدون وصف	تعديل الصلاحيات

فرق أمن المعلومات · 30-10-2026 23:34:37

إزالته من Domain Admins واستخدام صلاحيات مفوضة

INFRYX

لوحة المعلومات

جرد الحسابات

الحسابات الخاملة والقديمة

سياسة كلمات المرور

التوصيات

إعادة الاعتماد

استيراد بيانات AD

سجل التدقيق

الترخيص

الإعدادات

بيانات تجريبية

8 / 17

INFRYX
AD-GOV

INFRYX AD-GOV · v1.1

أدلة جاهزة للتدقيق بضغط واحدة

تسع أوراق

الغلاف والجرد وسياسة كلمات المرور وإعادة الاعتماد والمعالجة وسجل التدقيق الكامل.

الاعتماد والتوقيع

إعداد ومراجعة واعتماد من تقنية المعلومات والأمن والإدارة.

بلغتك

يصدر الملف بالعربية (RTL) أو الإنجليزية بحسب لغة الواجهة.



INFRYX-AD-Evidence.xlsx

حوكمة صلاحيات Active Directory - حزمة الأدلة

Sample Organization · corp.local · demo data

أهم الأرقام

154	إجمالي الحسابات
142	الحسابات المفعلة
4	الحسابات المميزة
7	حسابات الخدمة
29	حسابات مفعلة خاملة / لم تُستخدم
13	مفعلة وكلمة مرورها لا تنتهي
1	حسابات عالية الخطورة
10	حسابات (مميزة/خدمة/مدمجة) بدون مالك وغرض موثّقين

إعداد (تقنية المعلومات)

مراجعة (أمن المعلومات / الالتزام)

اعتماد (مدير أمن المعلومات / الإدارة)

4+

الحسابات الخاملة والقديمة

حسابات الخدمة

الحسابات المميزة

جرد الحسابات

الغلاف

التوصيات: من الملاحظات إلى الإجراء

ملاحظات من بياناتك أنت

مرتبة من الحرجة إلى المنخفضة، مع روابط للحسابات المتأثرة.

لماذا هي مهمة وماذا تفعل

تعليق واضح وخطوات تنفيذ وأوامر PowerShell.

قائمة تحصيل من 12 بنداً

LAPS و gMSA وسياسة التدقيق وتحصيل الـ Domain Controllers والنسخ الاحتياطي وغيرها.

متابعة كل بند

حالة ومبرر لكل بند، وكل تغيير يُسجّل في سجل التدقيق.



corp.local/recommendations

التوصيات

ملاحظات أمنية وتوصيات لتحسين بيئة Active Directory الخاصة بك. بناءً على بيانات استُوردت في 2026-10-30 23:34:36 (UTC).

3/12

تقدّم التحصيل

1

منخفضة · ملاحظات مفتوحة

5

متوسطة · ملاحظات مفتوحة

7

عالية · ملاحظات مفتوحة

1

حرجة · ملاحظات مفتوحة

الأولوية

الحالة

الكل

الكل

إعادة ضبط

تصفية

ملاحظات من بيانات AD الخاصة بك 15

تُكتشف تلقائيًا من آخر استيراد. حدث حالة كل بند لمتابعة المعالجة.

مفتوحة

الحسابات 1

حرجة Kerberos Pre-Authentication معطل

1

حساب معطل لا يتطلب Kerberos Pre-Authentication.

لماذا هذا مهم

أي شخص يصل إلى الـ Domain Controller يستطيع طلب AS-REP مشقّر لهذه الحسابات وكسر كلمة المرور (AS-REP Roasting) Offline دون أي بيانات دخول.

الإجراءات الموصى بها

1. ألق خيار 'Do not require Kerberos preauthentication': Set-ADAccountControl -Identity <sam> -DoesNotRequirePreAuth \$false

2. إذا كان هناك تطبيق قديم يحتاجه فعليًا، استخدم كلمة مرور عشوائية من 25 حرفًا أو أكثر وراقب الحساب.

3. غيّر كلمة مرور كل حساب متأثر لأن الـ Hash ربما تم التقاطه بالفعل.

الحسابات المتأثرة

svc_kerb

المراجع

MITRE ATT&CK T1558.004

افتح الصفحة المرتبطة

مفتوحة

ملاحظة / مبرر

تحديث

عالية

حسابات مميزة كلمة مرورها لا تنتهي

2

الصلاحيات المميزة

مفتوحة

عالية

تفويض غير مقيد (Unconstrained Delegation)

1

الحسابات

قيد التنفيذ

عالية

حسابات معطلة ما زالت في مجموعات مميزة

1

الصلاحيات المميزة

مفتوحة

بيانات تجريبية

INFRYX

حوكمة AD وإعادة الاعتماد

لوحة المعلومات

جرد الحسابات

الحسابات الخاملة والقديمة

سياسة كلمات المرور

التوصيات

إعادة الاعتماد

استيراد بيانات AD

سجل التدقيق

الترخيص

الإعدادات

الأمان مدمج في التصميم

تسجيل دخول محصّن



كلمة مرور أولية عشوائية تُغيّر إجباريًا، وقفل بعد 5 محاولات فاشلة، ومفتاح استرداد لمرة واحدة.

HTTPS افتراضيًا



Caddy بشهادة داخلية أو شهادتك أو Let's Encrypt، مع دعم IIS و nginx.

جمع بصلاحية قراءة فقط



يحتاج سكربت الجمع قراءة فقط ولا تُخزن أي بيانات اعتماد.

سجل تدقيق كامل



تُسجّل عمليات الدخول والاستيراد والقرارات والتصدير والإعدادات.

بيانات محمية



مجلد البيانات مقيّد على SYSTEM ومديري الجهاز المحليين فقط.

تحصين الويب



سياسة محتوى صارمة وحماية CSRF وملفات Cookie آمنة و HSTS.

تسجيل دخول عصري مع استرداد مدمج لكلمة المرور

نسيت كلمة المرور

تسجيل الدخول

العربية

الوضع الداكن

اعرف كل حساب.. وأثبت كل ضابط رقابي.

جرد الحسابات ومراجعة الصلاحيات المميزة وأدلة جاهزة للتحقق لبيئة Active Directory.

إعادة تعيين كلمة المرور

أدخل مفتاح الاسترداد واختر كلمة مرور جديدة.

اسم المستخدم

أدخل اسم المستخدم

مفتاح الاسترداد

XXXXX - XXXXX - XXXXX - XXXXX

كلمة المرور الجديدة (10 أحرف فأكثر)

تأكيد كلمة المرور الجديدة

إعادة تعيين كلمة المرور ←

ليس لديك مفتاح استرداد؟

العودة إلى تسجيل الدخول

إعادة الاعتماد

سياسة كلمات المرور

الحسابات الخاملة والقديمة

جرد الحسابات

يعمل بدون إنترنت

جاهز للتحقق

قراءة فقط

العربية

الوضع الداكن

اعرف كل حساب.. وأثبت كل ضابط رقابي.

جرد الحسابات ومراجعة الصلاحيات المميزة وأدلة جاهزة للتحقق لبيئة Active Directory.

مرحبًا بعودتك

سجل الدخول إلى لوحة INFRIX AD Governance

اسم المستخدم

admin

كلمة المرور

أدخل كلمة المرور

نسيت كلمة المرور؟

تسجيل الدخول ←

إعادة الاعتماد

سياسة كلمات المرور

الحسابات الخاملة والقديمة

جرد الحسابات

يعمل بدون إنترنت

جاهز للتحقق

قراءة فقط

إعادة التعيين من الخادم

كلمة مرور مؤقتة للطوارئ تُغيّر عند أول دخول.

نسيت كلمة المرور

إعادة تعيين بمفتاح استرداد لمرة واحدة، دون الحاجة إلى بريد إلكتروني.

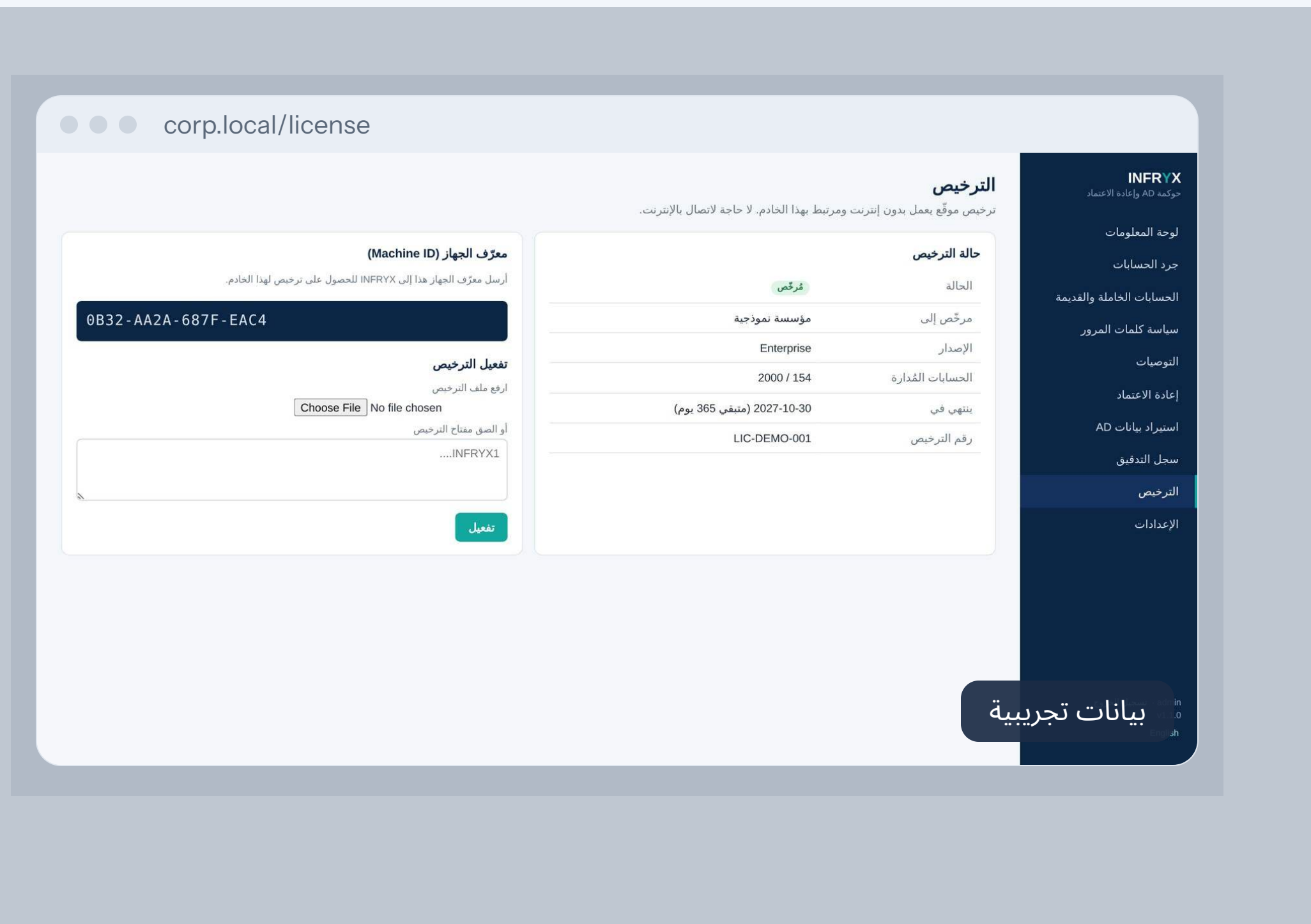
الوضع الفاتح والداكن

يُختار مرة واحدة ويحفظه المتصفح.

اختيار اللغة

عربي (RTL) أو إنجليزي من صفحة الدخول مباشرة.

ترخيص Offline وإصدارات مرنة



موقع ومرتبب بالجهاز



كل ترخيص مرتبط بـ Machine ID الخاص بالخادم، ولا يحتاج إنترنت.

Enterprise و Standard



تاريخ انتهاء وحد أقصى للحسابات المُدارة لكل ترخيص.

تجربة 14 يومًا



حتى 250 حسابًا، والملفات المصدّرة تحمل علامة مائية.

انتهاء سلس



7 أيام سماح ثم قراءة فقط. التجديد برفع ترخيص جديد دون المساس بالبيانات.

تركيب خلال دقائق

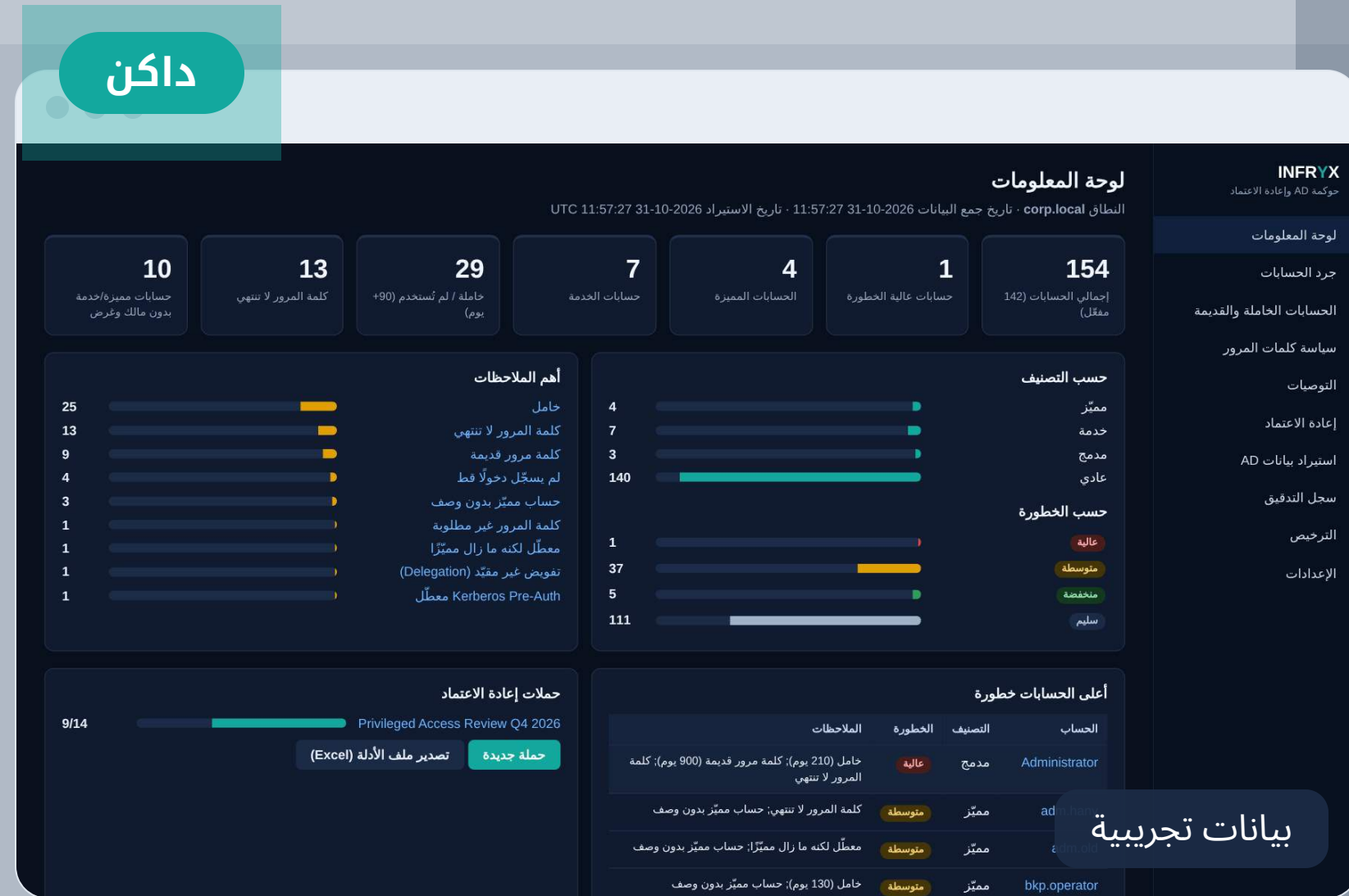
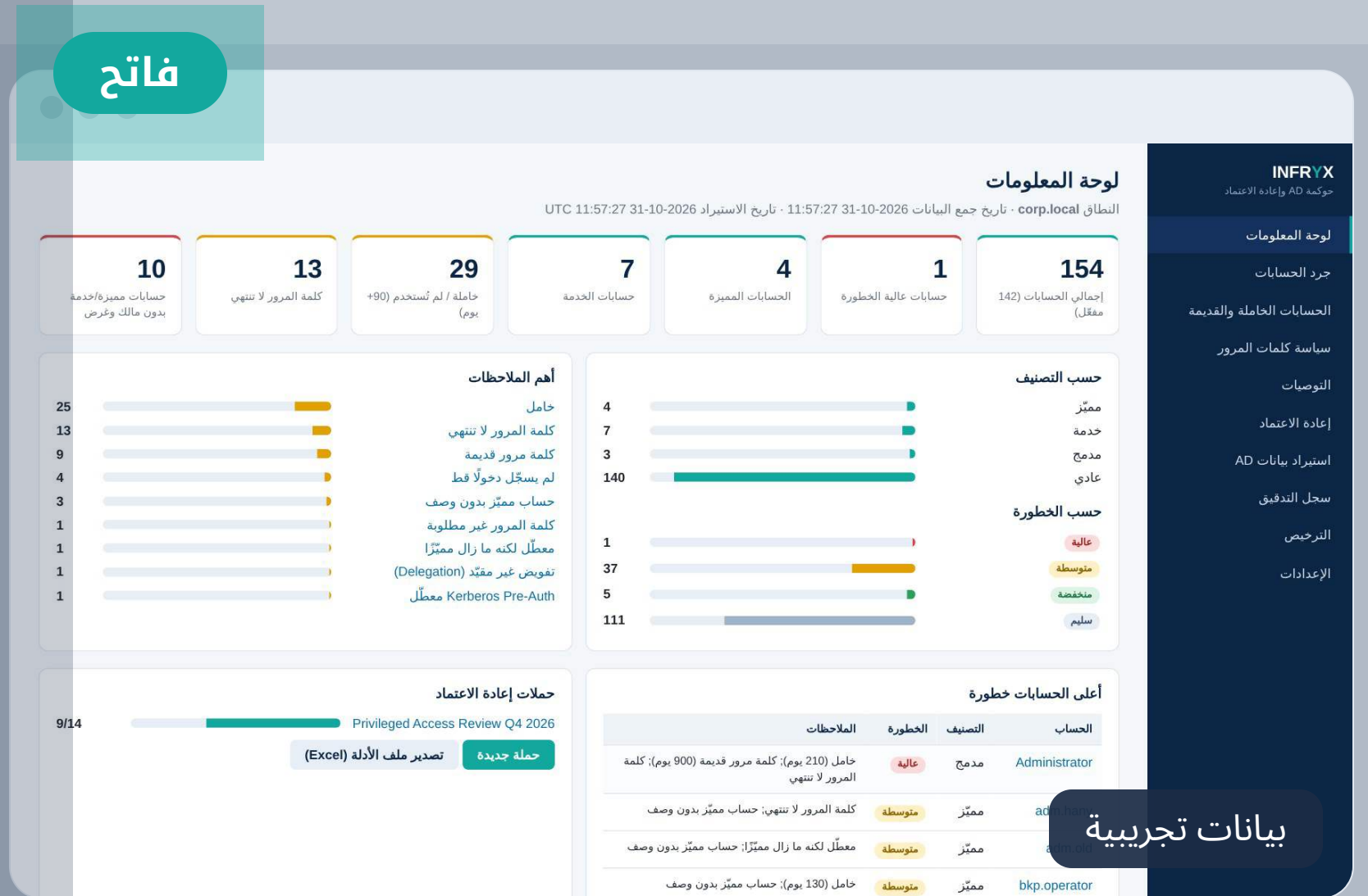


في نهاية التثبيت



• معرف الجهاز Machine ID • كلمة مرور المدير الأولية • رابط لفتح لوحة التحكم

وضع فاتح وداكن في كل النظام



تغطية كاملة



كل صفحة وجدول ورسم وشارة مهيّأة للوضع الداكن، والطباعة تبقى فاتحة.

يتبع نظامك



يبدأ بنمط Windows لديك إلى أن تختار.

مفتاح واحد يُحفظ

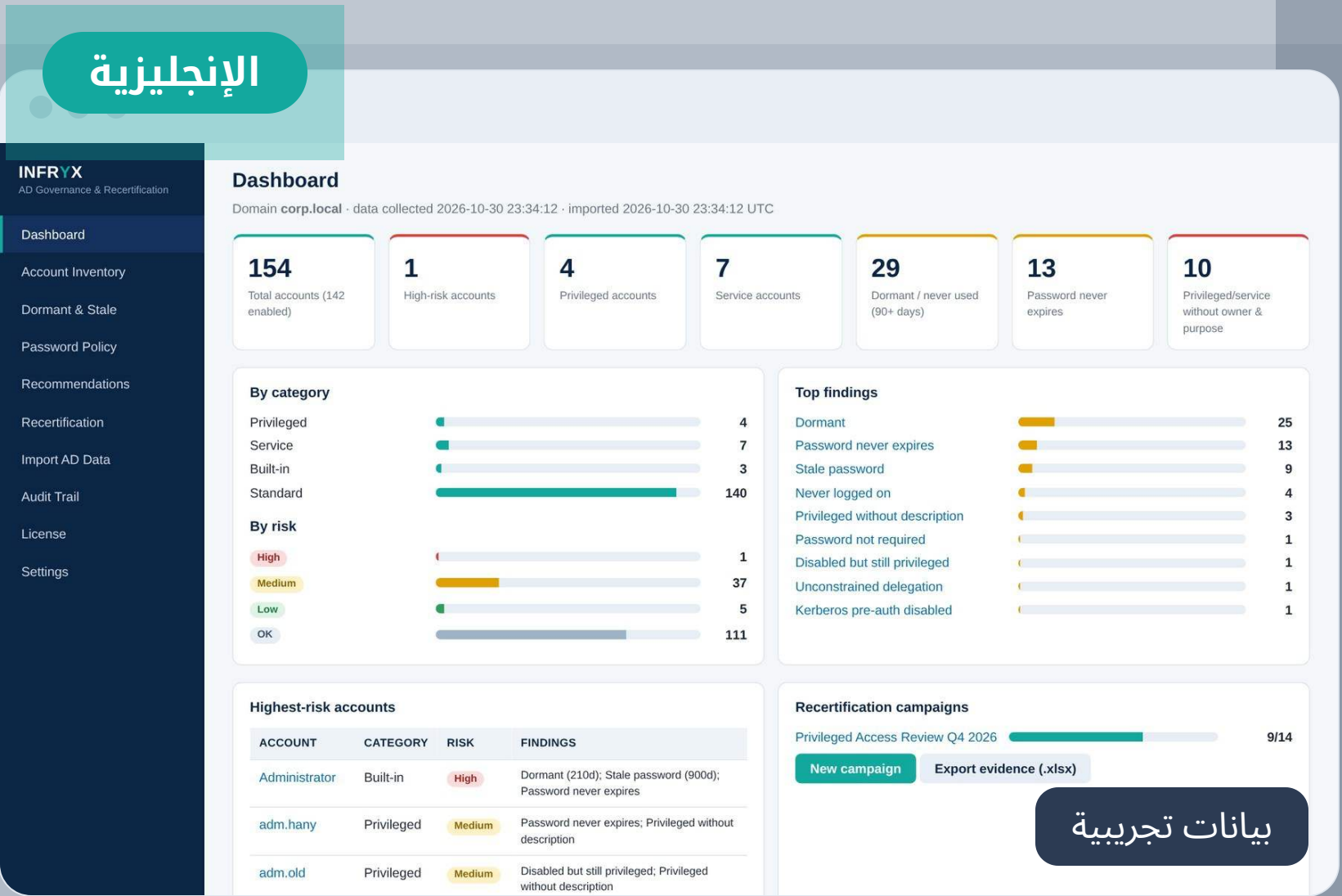
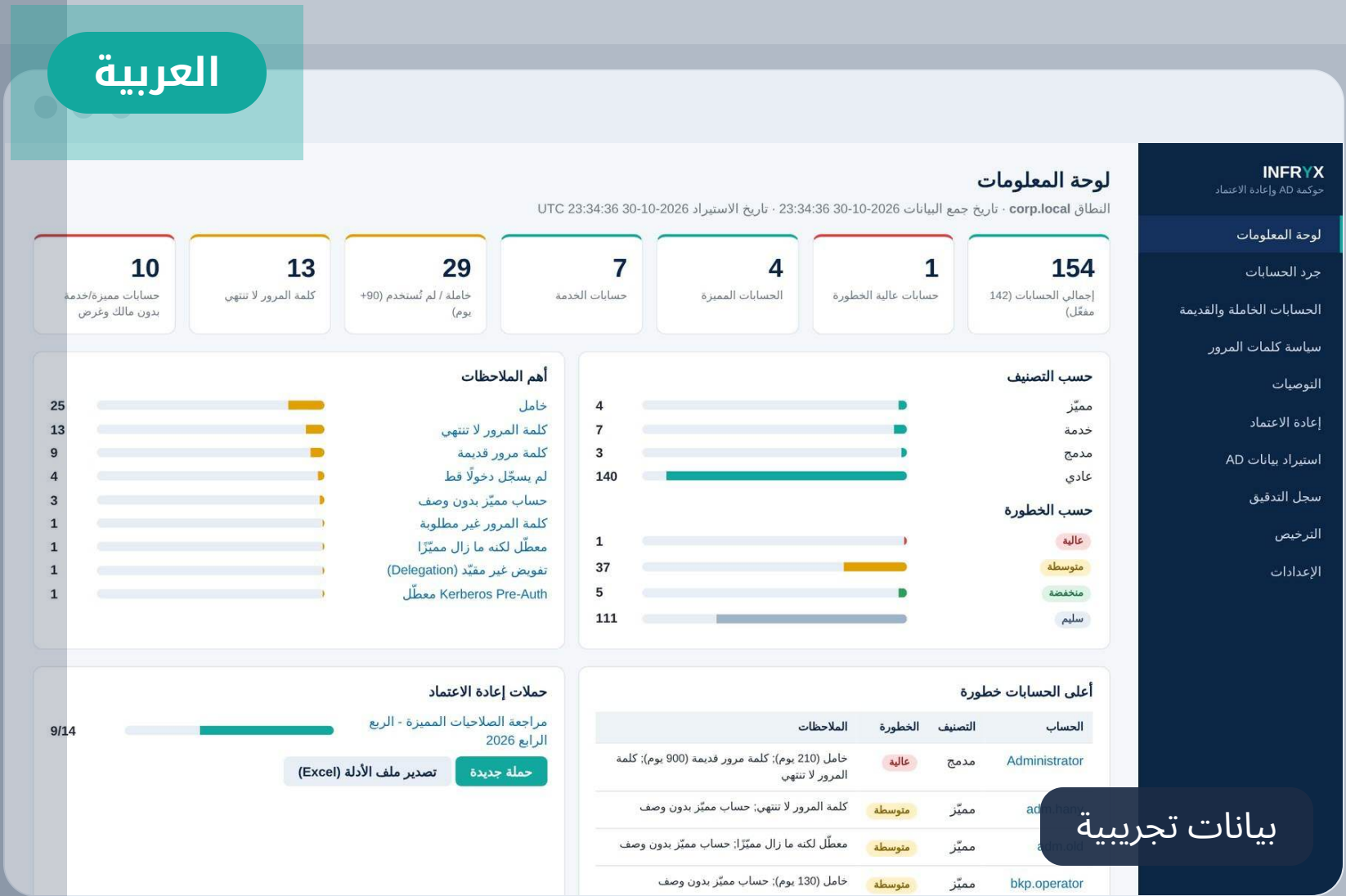


في القائمة الجانبية وصفحة الدخول، ويُحفظ لكل متصفح.

عربي وإنجليزي بضغطة واحدة

الإنجليزية

العربية



تبديل لكل مستخدم



لغة افتراضية عند التثبيت، ويستطيع كل مستخدم التبديل في أي وقت، حتى من صفحة الدخول.

الأدلة تتبع اللغة



ملف بالعربية أو الإنجليزية بحسب إعداد الواجهة.

عربية كاملة من اليمين إلى اليسار



كل صفحة ورسالة وتقرير مترجم.



اعرف من يملك الصلاحيات. وأثبت ذلك.

الإثبات

إعادة الاعتماد

الجرد

INFRYX AD-GOV · حوكمة AD وإعادة اعتماد الصلاحيات