



Product presentation · v1.1

AD Governance & Access Recertification

Know who has access to your Active Directory, and prove it to your auditors.

- Account inventory
- Risk analysis
- Access recertification
- Audit-ready evidence

corp.local

INFRYX
AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

Dashboard

Domain corp.local · data collected 2026-10-30 23:34:12 · imported 2026-10-30 23:34:12 UTC

154
Total accounts (142 enabled)

1
High-risk accounts

4
Privileged accounts

7
Service accounts

29
Dormant / never used (90+ days)

By category

Privileged4

Service7

Built-in3

Standard140

By risk

High1

Medium37

Low5

OK111

Highest-risk accounts

ACCOUNT	CATEGORY	RISK	FINDINGS
Administrator	Built-in	High	Dormant (210d); Stale password (900d); Password never expires
adm.hany	Privileged	Medium	Password never expires; Privileged without description
adm.old	Privileged	Medium	Disabled but still privileged; Privileged without description
bkp.operator	Privileged	Medium	Dormant (130d); Privileged without description
Guest	Built-in	Medium	Password not required
nessus	Service	Medium	Dormant (180d); Password never expires
endpoint-	Service	Medium	Password never expires; Unconstrained

Top findings

Dormant

Password never expires

Stale password

Never logged on

Privileged without description

Password not required

Disabled but still privileged

Unconstrained delegation

Kerberos pre-auth disabled

Recertification campaigns

Privileged Access Review Q4 2026

New campaign

Export evi

admin · Sign out

v1.1.0

العربية

Why Active Directory access needs governance



Hidden privileged access

Administrator rights sit inside nested groups that nobody reviews.



Forgotten accounts

Dormant and never-used accounts stay enabled for years.



No owner, no purpose

Service and shared accounts that nobody can explain to an auditor.



Weak password hygiene

Passwords that never expire and policies below the recommended baseline.



Evidence built by hand

Spreadsheets assembled under pressure before every audit.

One workflow, from raw AD data to audit evidence



1

Collect

A read-only PowerShell collector exports users, groups and the password policy.



2

Analyze

Every account is classified and scored for risk automatically.



3

Recertify

Owners review each account and record a decision.

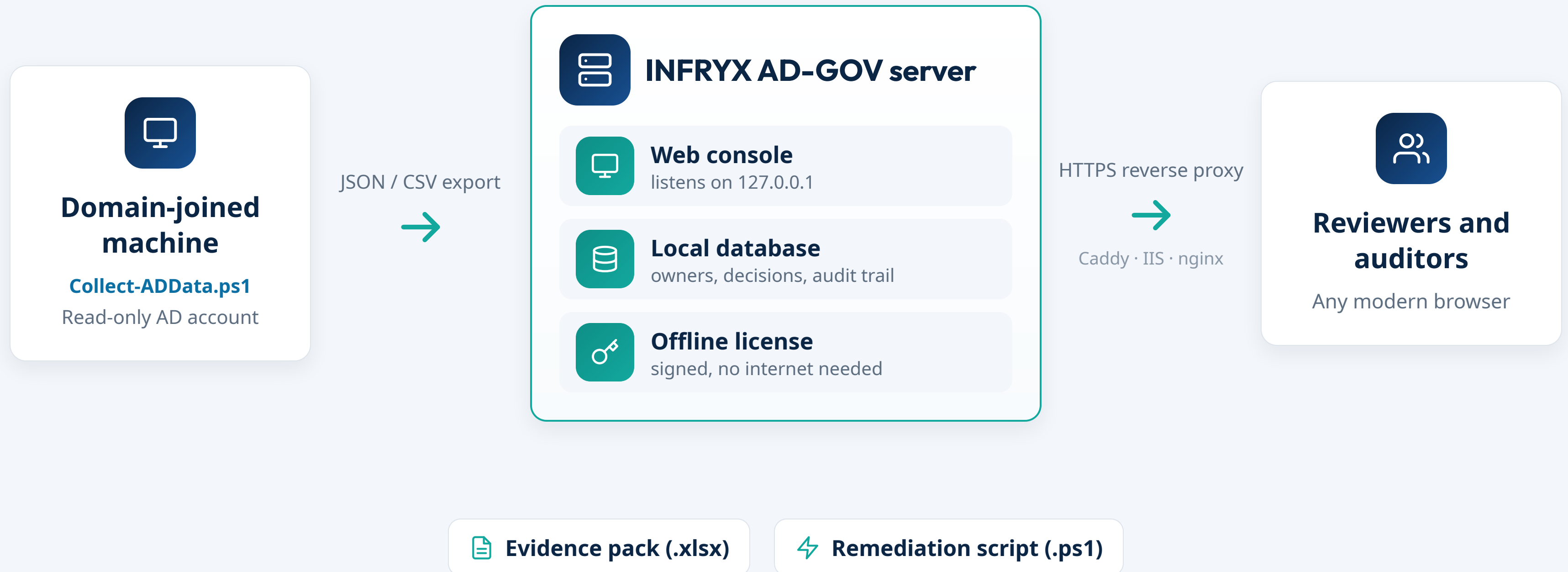


4

Prove

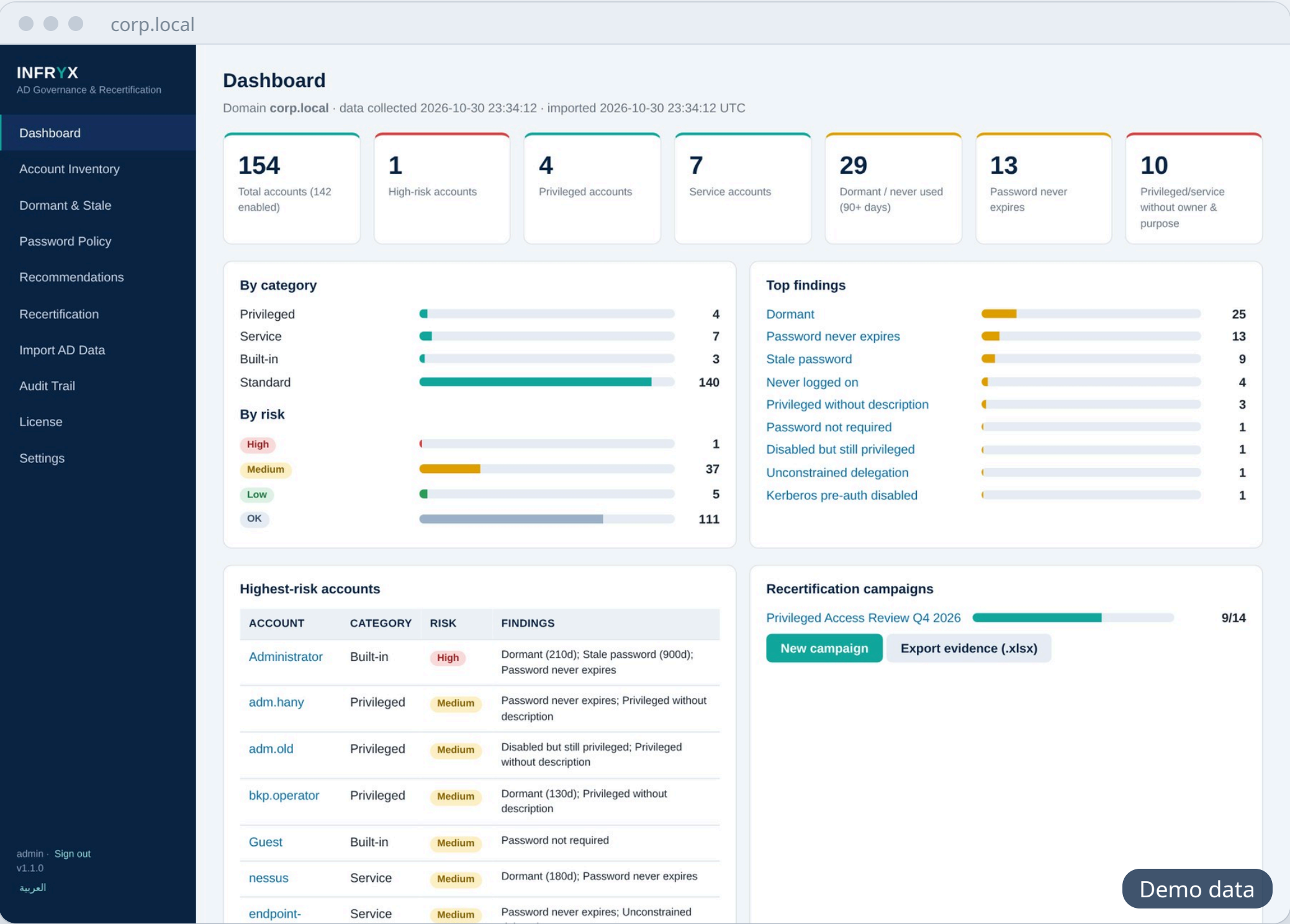
One click produces the Excel evidence pack for your auditors.

How it works



✓ On-premises: your data stays on your server ✓ No internet connection needed for licensing ✓ No credentials stored by the application

The state of your directory at a glance



Account inventory with automatic classification

corp.local

INFRYX
AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out
v1.1.0
العربية

Account Inventory

154 accounts match. Select accounts to assign owner / purpose in bulk.

Search

account, name, departmen

Category

All

Status

All

Risk

All

Owner & purpose

All

Filter

Reset

Business owner

e.g. Finance Manager

Owner email

Business purpose

Why does this account exist?

Category override

(keep)

Apply to selected

	ACCOUNT	CATEGORY	STATUS	LAST LOGON	OWNER	PURPOSE	RISK	FINDINGS
☐	Administrator Administrator	Built-in	Dormant	2026-04-03 210 days ago	—	—	High	Dormant (210d); Stale password (900d); Password never expires
☐	adm.hany Hany Adel (Admin)	Privileged	Active	2026-10-12 18 days ago	—	—	Medium	Password never expires; Privileged without description
☐	adm.old Old Admin	Privileged	Disabled	2025-09-25 400 days ago	—	—	Medium	Disabled but still privileged; Privileged without description
☐	bkp.operator Backup Operator	Privileged	Dormant	2026-06-22 130 days ago	—	—	Medium	Dormant (130d); Privileged without description
☐	endpoint-central Endpoint Central	Service	Active	2026-10-23 7 days ago	—	—	Medium	Password never expires; Unconstrained delegation
☐	Guest Guest	Built-in	Disabled	—	—	—	Medium	Password not required
☐	nessus Nessus Scanner	Service	Dormant	2026-05-03 180 days ago	—	—	Medium	Dormant (180d); Password never expires
☐	svc_kerb Kerberoast legacy	Service	Active	2026-10-12 18 days ago	—	—	Medium	Kerberos pre-auth disabled
☐	a.farouk92 Ahmed Farouk 92	Standard	Dormant	2026-06-07 145 days ago	—	—	Medium	Dormant (145d)
☐	a.hassan13 Amr Hassan 13	Standard	Active	2026-10-23 7 days ago	—	—	Medium	Stale password (664d); Password never expires

Demo data

- Privileged

Member (nested) of a privileged AD group, or AdminCount = 1
- Service

Has a Service Principal Name or a service-style name
- Built-in

Administrator, krbtgt, Guest and similar defaults
- Standard

Every other account

High · Medium · Low · OK

Risk is scored from the findings detected on each account.

Owner and purpose

Assign in bulk; every category override is audit-logged.

Dormant accounts and password hygiene

corp.local

INFRYX

AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out

v1.1.0

العربية

Dormant & Stale Accounts

Enabled accounts with no logon for 90+ days, never used, or password older than 365 days. Thresholds are in Settings. 37 found.

ACCOUNT	CATEGORY	LAST LOGON	PASSWORD AGE	OWNER	RISK	FINDINGS
o.gamal1 Omar Gamal 1	Standard	Never	33 days	—	Low	Never logged on
h.farouk14 Heba Farouk 14	Standard	Never	80 days	—	Low	Never logged on
n.fathy114 Nour Fathy 114	Standard	Never	21 days	—	Low	Never logged on
s.farouk124 Sara Farouk 124	Standard	Never	10 days	—	Low	Never logged on
r.gamal86 Rania Gamal 86	Standard	2025-09-10 (415d)	41 days	—	Medium	Dormant (415d)
o.samir137 Omar Samir 137	Standard	2025-09-25 (400d)	63 days	—	Medium	Dormant (400d)
a.nabil69 Ahmed Nabil 69	Standard	2025-11-11 (353d)	34 days	—	Medium	Dormant (353d)
m.zaki3 Mona Zaki 3	Standard	2025-11-15 (349d)	64 days	—	Medium	Dormant (349d)
h.said112 Hany Said 112	Standard	2025-11-15 (349d)	38 days	—	Medium	Dormant (349d)

Start a recertification campaign

Export evidence (.xlsx)

Demo data

Dormant and stale accounts

Enabled accounts with no sign-in for 90+ days (adjustable), never used, or with stale passwords.

corp.local

INFRYX

AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out

v1.1.0

العربية

Password Policy Report

Default domain policy and fine-grained policies compared with common baselines (NIST SP 800-63B / CIS).

Default Domain Policy

SETTING	CURRENT	RECOMMENDED	RESULT
Minimum password length	7	12 or more characters (NIST/CIS: 14 for privileged)	Review
Password history	24	24 passwords remembered	Compliant
Complexity enabled	True	Enabled	Compliant
Reversible encryption	False	Disabled	Compliant
Lockout threshold	5	Between 1 and 10 failed attempts	Compliant
Lockout duration (min)	30	15 minutes or more	Compliant

Max password age: 90 days · Min age: 1 days · Lockout window: 30 min.

Fine-grained policies (PSO)

NAME	PREC.	MIN LENGTH	HISTORY	MAX AGE	COMPLEXITY	LOCKOUT	APPLIES TO
PSO-Admins	10	14	24	60d	True	3	Domain Admins

Accounts with password exceptions

Password never expires

13

Administrator, adm.hany, svc_sql, svc_backup, ADSync ...

Password not required

1

Guest

Reversible encryption

0

Kerberos pre-auth disabled

1

svc_kerb

Stale password

9

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

Export evidence (.xlsx)

Demo data

Password policy report

Domain and fine-grained policies compared with NIST SP 800-63B / CIS style baselines.

Recertification campaigns

- 1 Choose scope → 2 Review each account → 3 Record the decision → 4 Close and lock

corp.local

INFRYX
AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out
v1.1.0
العربية

Campaigns

Privileged Access Review Q4 2026 Open

Due 2026-12-15 · scope: Privileged, Service, Built-in · 9 of 14 reviewed

Retain: 4

Modify access: 2

Disable: 3

Delete: 0

Pending: 5

All

Export evidence sheet (.xlsx)

Remediation script (.ps1, WhatIf by default)

☐ close even if items are pending

Close campaign

Decision for selected

Reviewer

Comment (required unless Retain)

Retain

Owner / manager name

Apply

☐	ACCOUNT	CATEGORY	RISK	OWNER / PURPOSE	FINDINGS AT REVIEW	DECISION
☐	Administrator Administrator	Built-in Domain Admins, Enterprise Admins, Schema Admins, Administrators	High	—	Dormant (210d); Stale password (900d); Password never expires	<div>Pending</div>
☐	Guest Guest	Built-in	Medium	—	Password not required	<div>Pending</div>
☐	endpoint-central Endpoint Central	Service	Medium	—	Password never expires; Unconstrained delegation	<div>Pending</div>
☐	svc_kerb Kerberoast legacy	Service	Medium	—	Kerberos pre-auth disabled	<div>Pending</div>
☐	krbtgt krbtgt	Built-in	OK	—		<div>Pending</div>
☐	adm.hany Hany Adel (Admin)	Privileged Domain Admins	Medium	—	Password never expires; Privileged without description	<div>Modify access</div> <div>Security Team · 2026-10-30 23:34:12 Remove from Domain Admins, use delegated rights</div>
☐	adm.old	Privileged	Medium	—	Disabled but still privileged; Privileged	<div>Disable</div>

Four decisions

Retain · Modify access · Disable · Delete

Consistent evidence

A snapshot of the selected accounts is frozen inside the campaign.

Accountability

Reviewer, date and a comment for every decision other than Retain.

Safe remediation

A PowerShell script is generated in WhatIf mode by default.

Audit-ready evidence in one click

✕ INFRYX-AD-Evidence.xlsx

Active Directory Access Governance - Evidence Pack

Sample Organization · corp.local · demo data

Key figures

Total accounts	154
Enabled accounts	142
Privileged accounts	4
Service accounts	7
Dormant / never-used enabled accounts	29
Enabled with password never expires	13
High-risk accounts	1
Privileged / Service / Built-in without owner & purpose	10

Prepared by (IT)

Reviewed by (Security / Compliance)

Approved by (CISO / Management)

Cover

Account Inventory

Privileged Accounts

Service Accounts

Dormant & Stale

+4



Nine sheets

Cover, inventories, password policy, recertification, remediation and the full audit trail.



Sign-off block

Prepared, reviewed and approved by IT, Security and management.



Your language

The workbook is issued in Arabic (RTL) or English, matching the console.

Recommendations: from findings to action

INFRYX
AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out

v1.1.0

العربية

corp.local/recommendations

Recommendations

Security findings and hardening recommendations for your Active Directory. Based on data imported at 2026-10-30 23:34:12 UTC.

1
Critical · open findings

7
High · open findings

5
Medium · open findings

1
Low · open findings

3/12
Hardening progress

Priority

All

Status

All

Filter

Reset

Findings from your AD data

15

Detected automatically from the latest import. Update the status of each item to track the remediation.

▼

Critical

Kerberos pre-authentication is disabled

1

Accounts

Open

1 enabled account(s) do not require Kerberos pre-authentication.

WHY IT MATTERS

Anyone who can reach a domain controller can request an encrypted AS-REP for these accounts and crack the password offline (AS-REP roasting) without any credentials.

RECOMMENDED ACTIONS

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

2. If a legacy application really needs it, use a random password of 25+ characters and monitor the account.

3. Reset the password of each affected account, because the hash may already have been captured.

AFFECTED ACCOUNTS

svc_kerb

REFERENCES

MITRE ATT&CK T1558.004

Open related view

Open

Note / justification

Update

►

High

Privileged accounts whose password never expires

2

Privileged access

Open

►

High

Unconstrained delegation

1

Accounts

In progress

►

High

Disabled accounts still in privileged groups

1

Privileged access

Open

Findings from your own data

Ranked from Critical to Low, with the affected accounts linked.

Why it matters, and what to do

Clear reasoning, step-by-step actions and PowerShell commands.

12-point hardening checklist

LAPS, gMSA, audit policy, domain controller hardening, backup and more.

Track every item

Status and justification per item; each change is audit-logged.

Demo data

INFRYX AD-GOV · v1.1

10 / 15

Security built in



Read-only collection

The collector needs read access only. No credentials are stored.



HTTPS by default

Caddy with an internal CA, your own certificate or Let's Encrypt; IIS and nginx supported.



Hardened sign-in

Random initial password with forced change, and lockout after 5 failed attempts.



Web hardening

Strict content security policy, CSRF protection, secure cookies and HSTS.



Protected data

The data folder is restricted to SYSTEM and local Administrators.



Full audit trail

Sign-ins, imports, decisions, exports and settings are all logged.

Offline licensing, flexible editions

- 

Signed and machine-bound

Each license is tied to the server's Machine ID. No internet connection is needed.
- 

Standard and Enterprise

Expiry date and managed-account limit set per license.
- 

14-day trial

Up to 250 accounts, with watermarked exports.
- 

Graceful expiry

7 days of grace, then read-only. Renew by uploading a new license; data is untouched.

corp.local/license

INFRYX

AD Governance & Recertification

Dashboard

Account Inventory

Dormant & Stale

Password Policy

Recommendations

Recertification

Import AD Data

Audit Trail

License

Settings

admin · Sign out

v1.1.0

العربية

License

Offline signed license bound to this server. No internet connection is required.

License status

Status	Licensed
Licensed to	Sample Organization
Edition	Enterprise
Managed accounts	154 / 2000
Expires	2027-10-30 (365 day(s) left)
License ID	LIC-DEMO-001

Machine ID

Send this Machine ID to INFRYX to receive a license for this server.

0B32-AA2A-687F-EAC4

Activate license

Upload license file (.lic)

Choose File

No file chosen

or paste the license key

INFRYX1....

Activate

Demo data

Deploy in minutes

1

Run the installer

Windows setup wizard
(x64).

2

Choose address, HTTPS and language

Server DNS name, HTTPS
mode and default
language.

3

Services start automatically

Startup tasks with auto-
restart, plus a firewall
rule.

4

Activate the license

Send the Machine ID,
upload the .lic file.

5

Collect, import, review

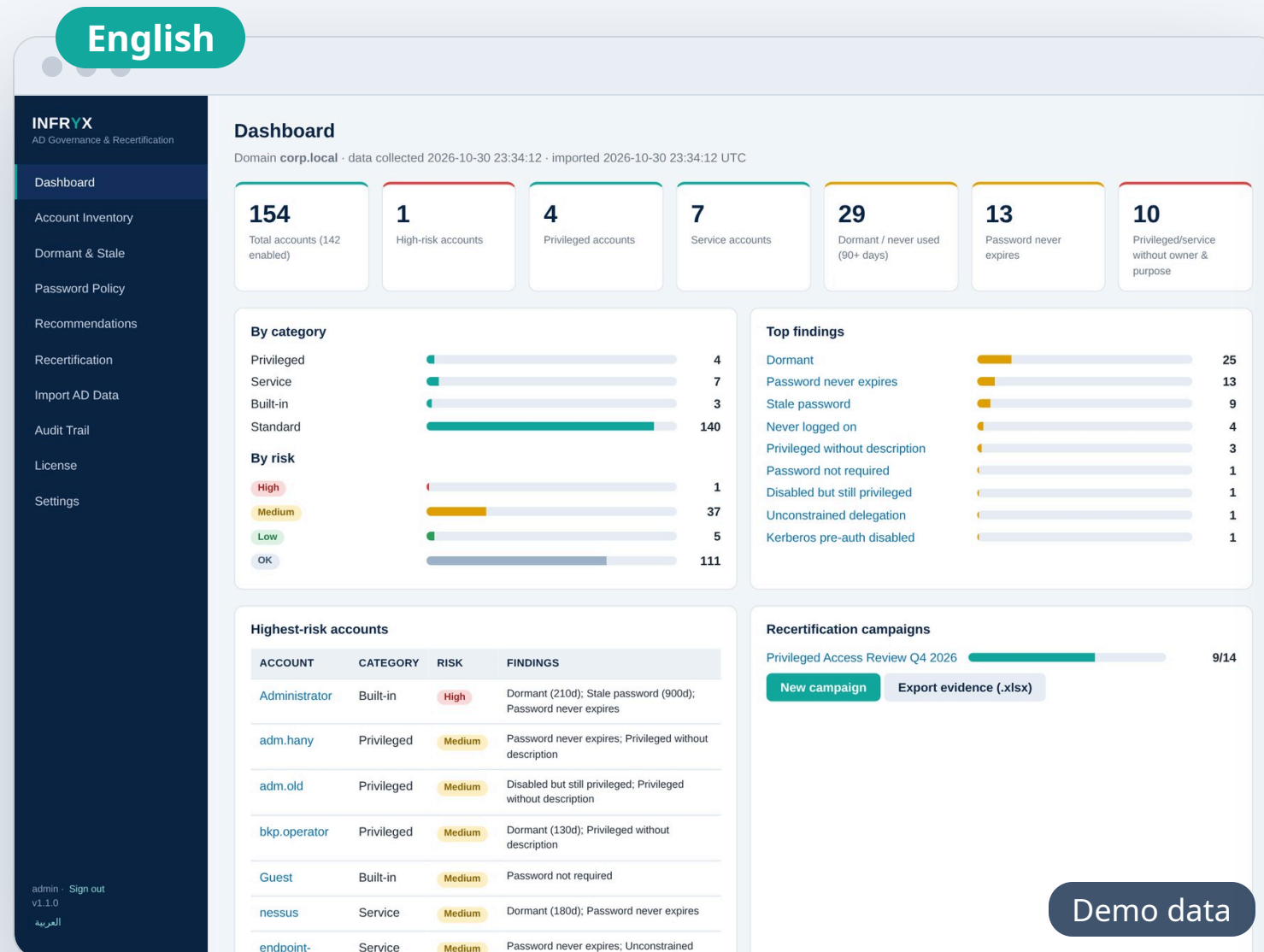
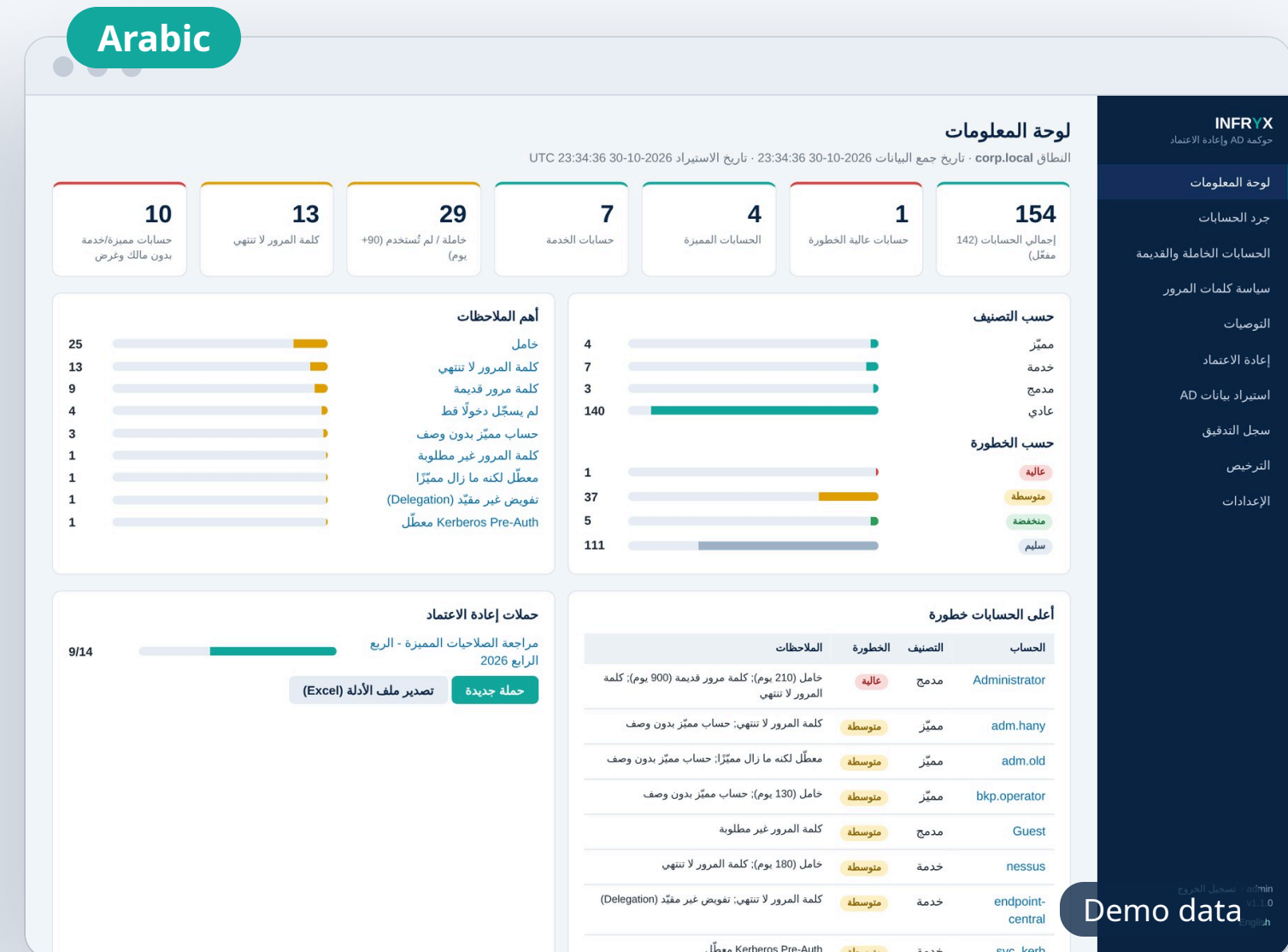
Run the collector, import
the file and open your
first campaign.



At the end of setup

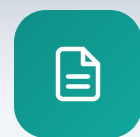
- Your Machine ID
- The initial administrator password
- A link that opens the console

Arabic and English, one click apart



Full right-to-left Arabic

Every page, message and report is translated.



Evidence follows the language

Arabic or English workbook, as the console is set.



Per-user switch

Default language set at install; each user can switch at any time.



Know who has access. Prove it.

Inventory

Recertify

Prove

INFRYX AD-GOV · AD Governance & Access Recertification