Hisn user guide

Active Directory security console for Hisn 1.32 and later: install, scan, read the results, monitor and report.

English | العربية

1. What Hisn does

Hisn assesses the security of Active Directory and the Windows servers in it, tracks every finding until it is fixed, and watches the domain controllers for attacks and for changes to the most sensitive (Tier 0) objects. It is one Windows service with a web console.

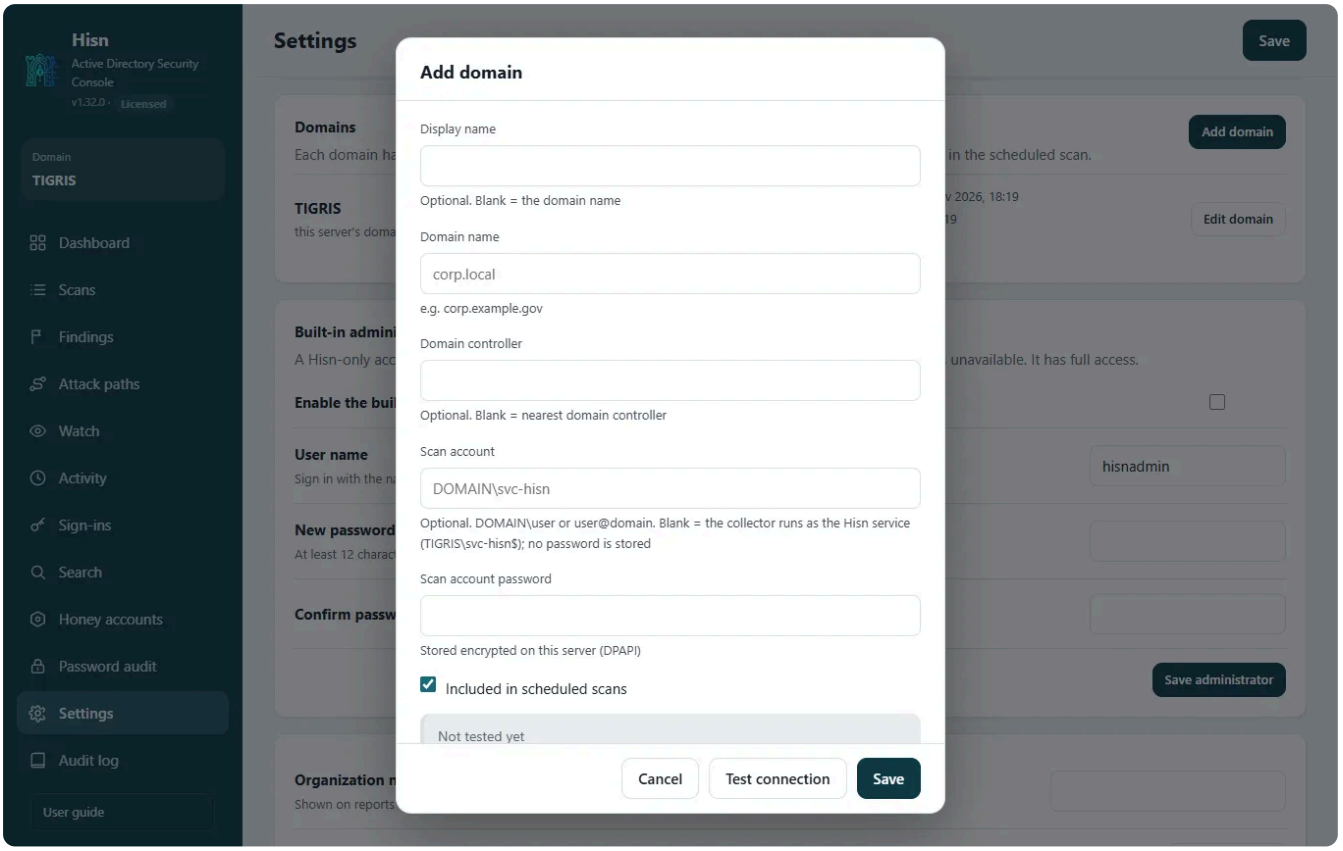
- **Read-only.** Hisn never writes to Active Directory, Group Policy or servers, and installs nothing on domain controllers. Fix and rollback scripts are generated for an administrator to review and run.
- **Offline.** No internet connection is needed to run or to activate it. Updates arrive as signed files you copy in.
- **No password hashes.** Hisn never reads or stores hashes. The optional password audit runs separately, and Hisn imports only account names.
- **Arabic and English** throughout the console, the reports and this guide.

2. Quick start

From a new installation to your first results in five steps. Each step links to its full section.

1. **Install** `Hisn-Setup-v<version>.exe` on a domain-joined server and finish with *Open the Hisn console* ticked (section 4).
2. **Sign in** with your domain account (a member of **Hisn-Admins**) or the built-in administrator you created in Setup (section 5).
3. **Check the domain** in *Settings* → *Domains*. Setup adds the server's own domain; open it with **Edit domain** and press **Test connection** (section 7).

4. **Run a scan**: *Scans* → *Run scan*, or the scan button on the dashboard. A medium domain takes 1 to 5 minutes.
5. **Read the dashboard**, then open *Findings* and start with the highest severity (section 8).



Step 3: the domain form. Blank fields are optional; **Test connection** checks what the scan will need.

3. Requirements

Item	Requirement
Server	Windows Server 2016 or later, joined to the domain. A domain controller is the simplest choice; a member server works with the RSAT "Active Directory module for Windows PowerShell".
PowerShell	5.1 (included in Windows Server 2016 and later).
Browser	Microsoft Edge, Chrome or Firefox. **Internet Explorer is not supported.** It is the only browser on Server 2016/2019, so open the console from your own PC or install Edge or Chrome on the server.
Disk	About 300 MB for the program; scan history grows by 1 to 5 MB per scan for a medium domain. Older scans' raw data is kept compressed. No scan or backup starts when free space is below 2 GB (a setting).
Memory	The collector runs in PowerShell on the Hisn server and needs about 1 GB free for a directory of 20,000 accounts (measured, see below); allow more for larger directories.
Network from the Hisn server	To the DCs: LDAP 389, Global Catalog 3268, AD Web Services 9389, SMB 445 (SYSVOL), RPC 135 and dynamic ports, WinRM 5985. To member servers: WinRM 5985. To CAs: RPC and HTTP/HTTPS. To the console from administrators' PCs: HTTPS 8443 (configurable).

Measured scan size

Measured on a lab domain controller (a virtual machine, one DC, the collector running on the DC itself), with synthetic disabled accounts, computer objects and nested groups added to the lab domain. Member servers were not scanned.

Directory	Collection	Collector peak memory	Analysis	Collected data
20,017 users / 5,001 computers / 557 groups	6 minutes	981 MB	5 s / 226 MB	62 MB

Each member server adds a WinRM round trip (up to 300 per scan); DCs reached over a slow link add to the collection time. Real directories carry more attributes per account than the synthetic ones, so use these figures as a lower bound.

4. Install and upgrade

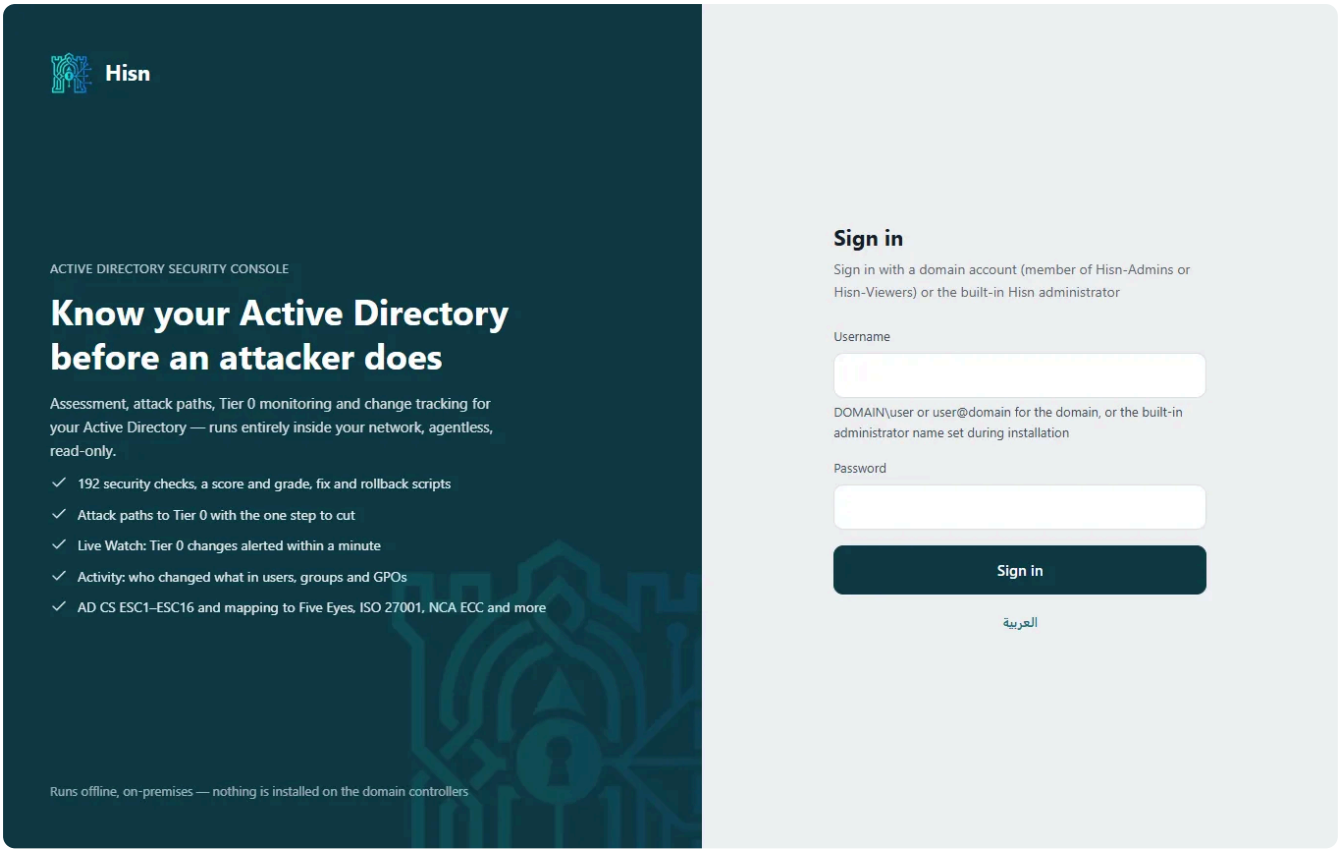
1. Copy `Hisn-Setup-v<version>.exe` to the server and run it as an administrator. Check its SHA-256 against the value published with the download. If SmartScreen appears, choose *More info* → *Run anyway*.
2. Choose the language, accept the licence, then set the options: HTTPS port (default 8443) and who may open the console (administrators on the network, or this server only).
3. Create the **built-in administrator** (a Hisn-only account for when domain sign-in is unavailable) and set the first domain.
4. Finish with *Open the Hisn console* ticked. The first start can take up to 2 minutes while the HTTPS certificate is created.

Setup creates the service `HisnConsole` (LocalSystem, automatic start), the AD groups **Hisn-Admins** and **Hisn-Viewers** (and adds you to Hisn-Admins), a firewall rule for the console port, and a Start menu folder. The program goes under `C:\Program Files\Hisn`; Setup refuses a folder outside Program Files.

Upgrade: run the new Setup over the existing installation. History, settings, domains, licence and finding states are kept. Setup backs up the data before it changes anything, stops if that backup fails, and refuses to install an older version over a newer one. Silent install: `Hisn-Setup-v<version>.exe /S`.

5. Sign in and access

Open `https://<server>:8443`. The browser warns about the self-signed certificate on first use; choose *Advanced* → *Continue*, or install your own certificate in `C:\ProgramData\Hisn\tls`.



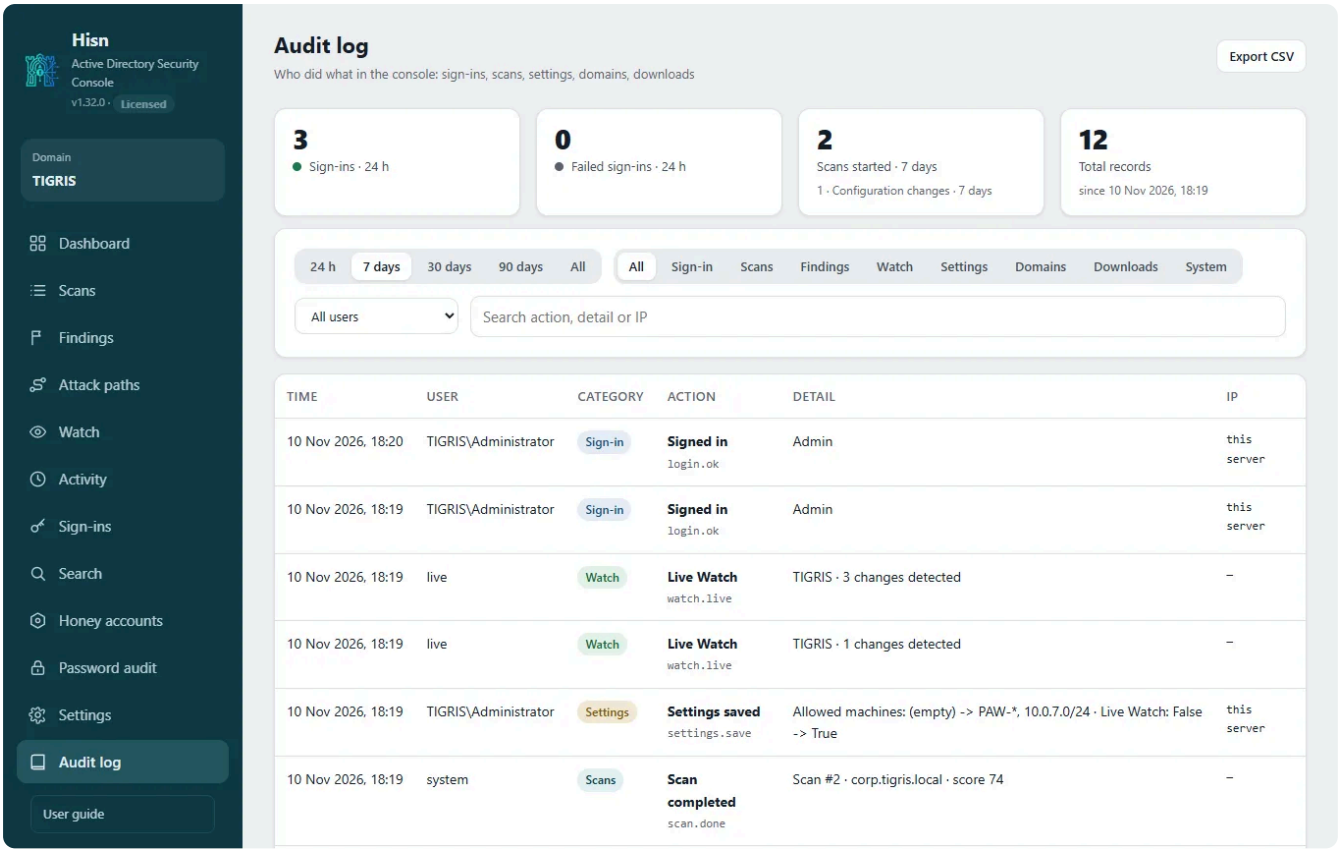
The sign-in page. Use `DOMAIN\user` or `user@domain`, or the built-in administrator's name. The link under the button switches the language.

Who	Can
Members of **Hisn-Admins**	Run scans, manage findings, download fix scripts, change settings, import content and licences.
Members of **Hisn-Viewers**	View the dashboard, findings, Watch, activity and reports.
Built-in administrator	Everything; locked for 15 minutes after 10 wrong passwords.

Sessions end after 30 minutes idle or 12 hours. Five wrong passwords from the same user and address lock that sign-in for 15 minutes.

At the bottom of the sidebar: **ع / EN** switches the language, and the theme button cycles *Auto* (follows Windows), *Light* and *Dark*; the choice is kept in this browser. On a phone the sidebar folds into the menu button at the top. Every page works with the keyboard: Tab moves, Enter or Space opens a row, Escape closes a dialog, and a *Skip to content* link is the first stop.

Audit log. Every sign-in and every change made in the console (settings, finding states, exports, restores) is recorded on the *Audit log* page, with the user and address. Admins can filter it and export it as CSV.



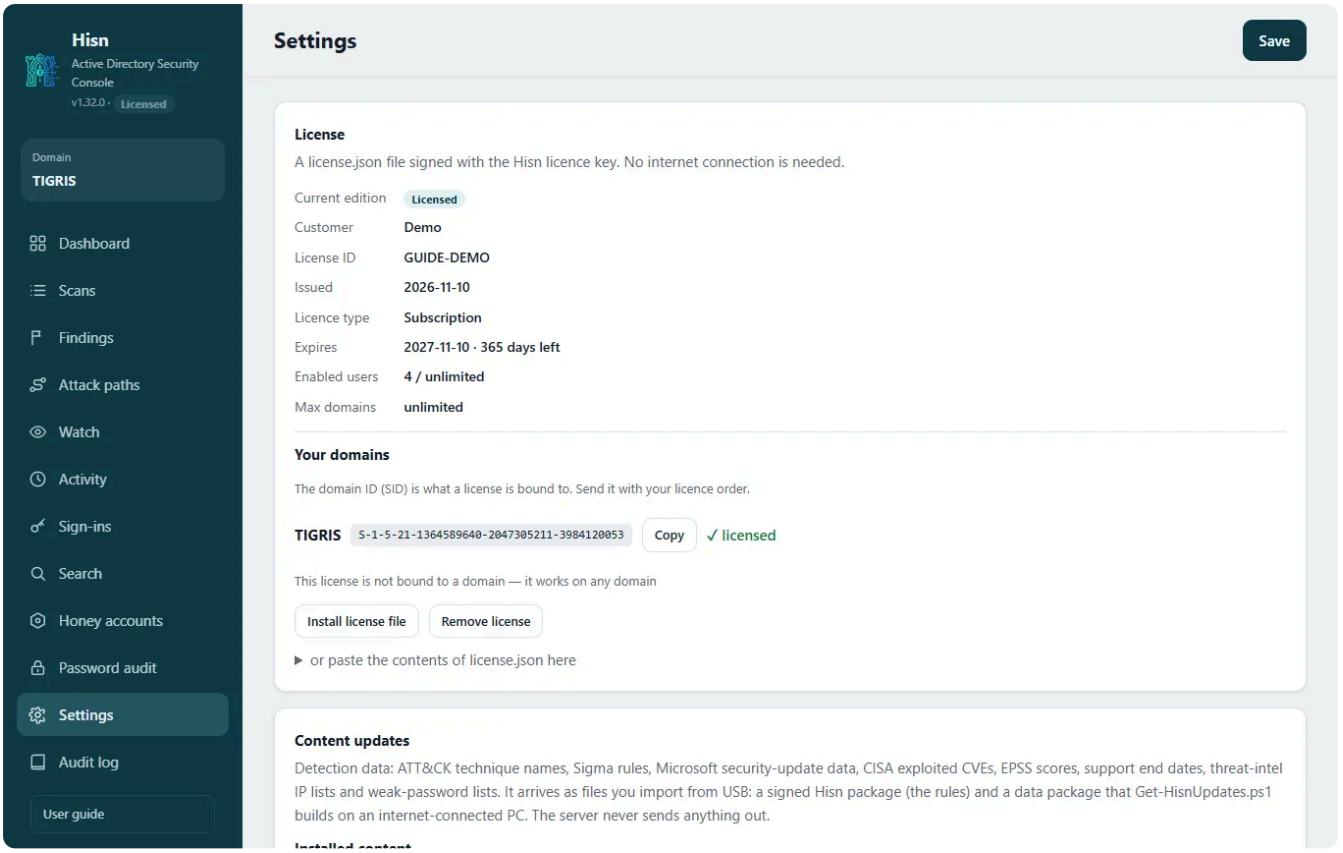
The Audit log: who did what in Hisn itself.

---

6. Licence

Without a licence Hisn runs in **demo** mode: one full scan of one domain, with every result and report for that scan. Ongoing features (schedules, history, several domains, Watch, Live Watch, alerts, branding, content updates, SIEM) need a licence.

Install the `license.json` you receive in *Settings → License → Install license file*, or paste its contents. The card shows the edition, licence type, expiry, enabled users and maximum domains. Under *Your domains* it shows each domain's ID (SID): send it with a licence order, because a licence is bound to domain IDs, not to a server.



Settings → License. Copy the domain ID for a licence order; install the file you receive with **Install license file**.

Type	Behaviour
Subscription	Works until the end date, then 14 more days with a warning, then read-only (past results stay viewable).
Perpetual with maintenance	Never expires for the versions released before the maintenance date. Newer versions and new content packages need renewed maintenance.
Trial	14 days, full features.

Size tiers count enabled users (S 1,000 · M 5,000 · L 20,000 · XL unlimited). Going over shows a warning; it never blocks scanning.

---

7. Domains and scan accounts

Add each domain in *Settings → Domains → Add domain* (picture in Quick start): the DNS name, optionally a preferred DC, and optionally a scan account (`DOMAIN\user` ; the password is stored encrypted with Windows DPAPI). Leave the account blank to scan as the Hisn service;

the form names the identity the service runs as. On a DC running as LocalSystem, that reaches other machines as the DC's computer account (`DOMAIN\DC$`).

Press **Test connection**. It checks four things and explains any failure:

Test	Needed for	Rights
Directory read (LDAP)	Almost every check	Any domain user
Remote PowerShell (WinRM) to the PDC	DC settings: signing, SMB, spooler, LSA protection, audit policy, firewall, patches	Domain Admins (an administrator of the DCs). Remote Management Users alone lets the account connect but not read these settings; Hisn then shows them as not evaluated
Security log	"Changed by" in Watch, Live Watch, sign-ins and lockouts	Event Log Readers on the DCs
SYSVOL	GPO content and settings, scripts, secrets in SYSVOL	Any domain user

Member servers (checks S-001 to S-015 and admin sessions) are read over WinRM and need the scan account (or the DC's computer account when no account is set) in each server's local Administrators group. Up to 300 servers are read per scan.

For a domain in another forest, use an account of that domain; the trust must allow it.

Run the service as a gMSA (recommended)

By default the Hisn service runs as LocalSystem. That works, but on a domain controller it scans as the DC's own computer account, and a scan account typed into Settings is a password stored on the server. A **group managed service account** (gMSA) avoids both: Windows creates and rotates its password, only the Hisn server can use it, and Hisn stores nothing.

Run these on a DC as a Domain Admin (Hisn never runs them itself). Replace `HISNSERVER` with the name of the server Hisn is installed on; Setup also writes this list, with your names filled in, to `C:\ProgramData\Hisn\Create-Hisn-gMSA.txt` .

```
# 1. once per forest - skip if Get-KdsRootKey already returns a key
Add-KdsRootKey -EffectiveImmediately          # then wait 10 hours for it to rep
# (single-DC lab only:  Add-KdsRootKey -EffectiveTime ((Get-Date).AddHours(-10))

# 2. the account - only the Hisn server may fetch its password
New-ADServiceAccount -Name svc-hisn -DNSHostName svc-hisn.corp.example `
    -PrincipalsAllowedToRetrieveManagedPassword 'HISNSERVER$'

# 3. the read rights from the table above
Add-ADGroupMember 'Event Log Readers'       -Members 'svc-hisn$'
Add-ADGroupMember 'Remote Management Users' -Members 'svc-hisn$'
```

Then on the Hisn server, as administrator:

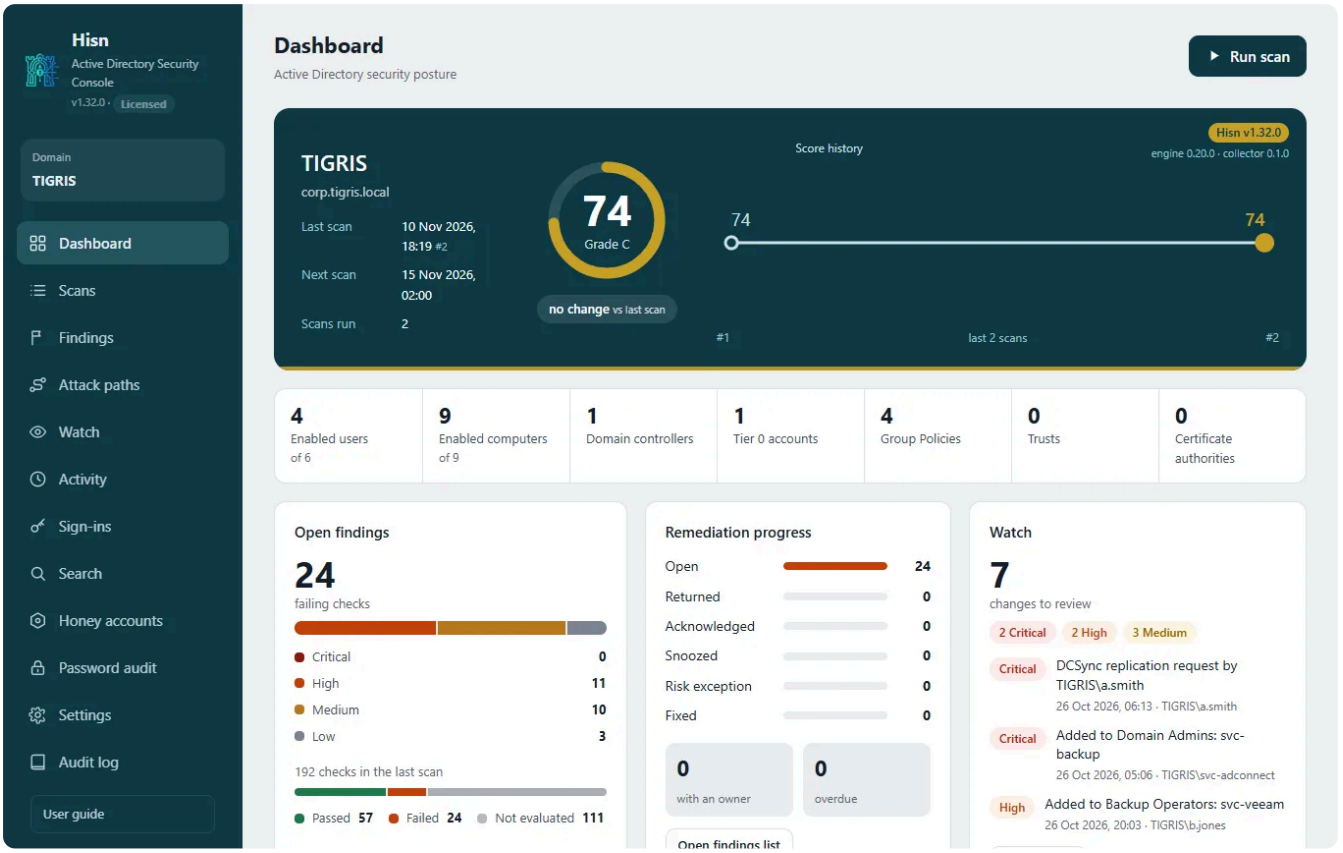
```
Install-ADServiceAccount svc-hisn
Test-ADServiceAccount svc-hisn      # must print True
```

Run Setup again (it keeps your data) and enter `CORP\svc-hisn$` under *Run as gMSA*, or run `Install-HisnConsole.ps1 -ServiceAccount CORP\svc-hisn$`. Setup checks the account with `Test-ADServiceAccount`, gives it rights on `C:\ProgramData\Hisn`, and restarts the service. In *Settings* → *Domains*, leave the scan account blank for every domain the gMSA can read.

- **Other domains and forests.** Group membership is per domain: add `svc-hisn$` to Event Log Readers and Remote Management Users in each child domain or trusting forest, or keep a scan account for that domain.
- **Member-server checks** still need the account in each server's local Administrators group, as for any scan account.
- **Domain controller settings** (signing, SMB, spooler, LSA protection, audit policy, updates, dcdiag) need an administrator of the DCs. In Remote Management Users the gMSA can connect but not read them, so those checks show as not evaluated: set a scan account in Domain Admins for the domain (Domains page) to assess them.
- **Moving to a new server** means adding the new server to `PrincipalsAllowedToRetrieveManagedPassword` (`Set-ADServiceAccount svc-hisn -PrincipalsAllowedToRetrieveManagedPassword 'NEWSERVER$'`). A backup restored there needs no passwords re-entered.

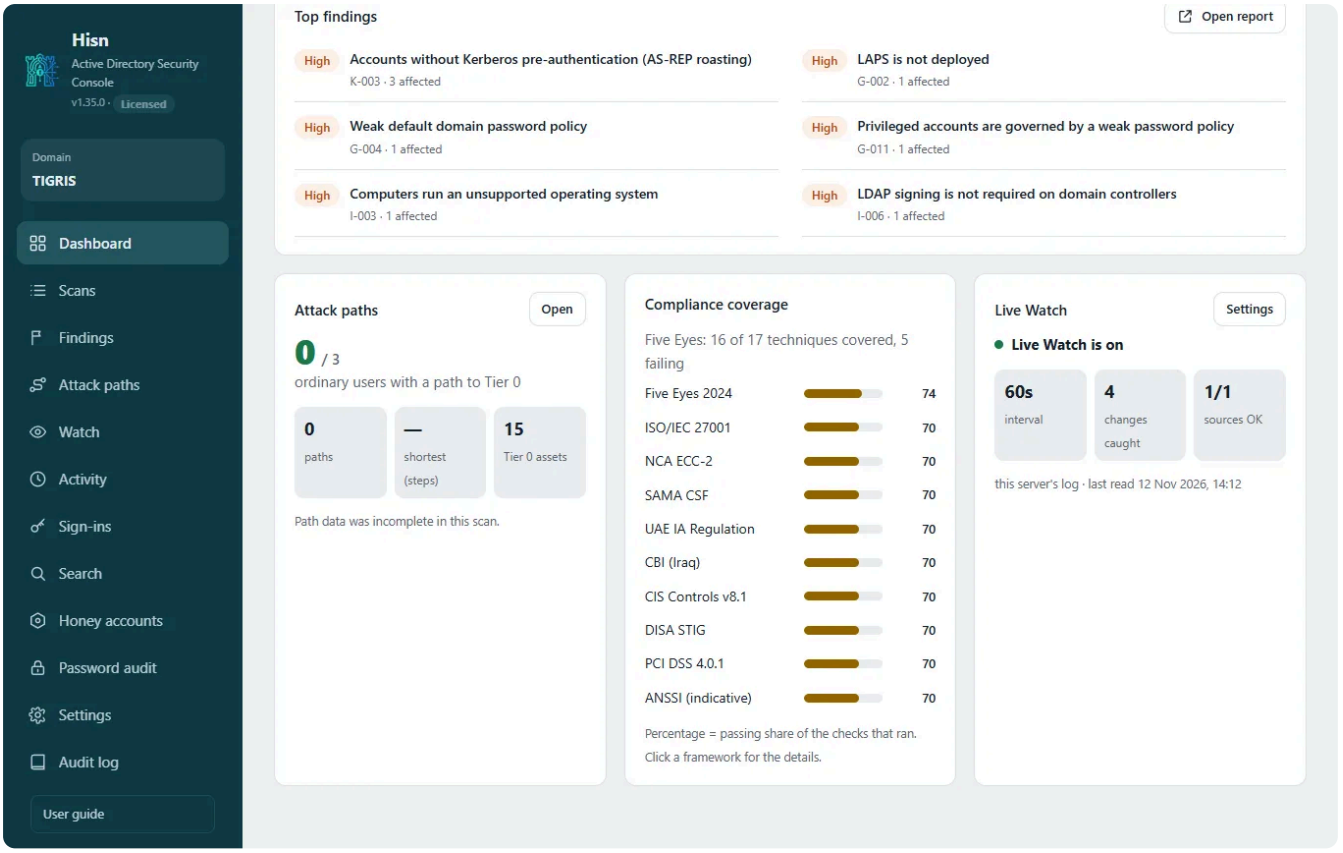
8. The dashboard

The dashboard is the domain's state at a glance. The domain shown is the one selected in the box at the top of the sidebar.



The upper half of the dashboard.

1. **Score and grade** (0 to 100, A to F), the change since the previous scan, and the score trend over the latest scans.
2. **The last and next scan**, and how many scans this domain has.
3. **Domain counts**: enabled users and computers, DCs, Tier 0 accounts, GPOs, trusts and certificate authorities.
4. **Open findings** by severity, and how many of all checks passed, failed or could not be evaluated in the last scan.
5. **Remediation progress**: findings open, returned, acknowledged, snoozed, under a risk exception or fixed; and how many have an owner or are overdue.
6. **Watch**: changes waiting for review, newest first.



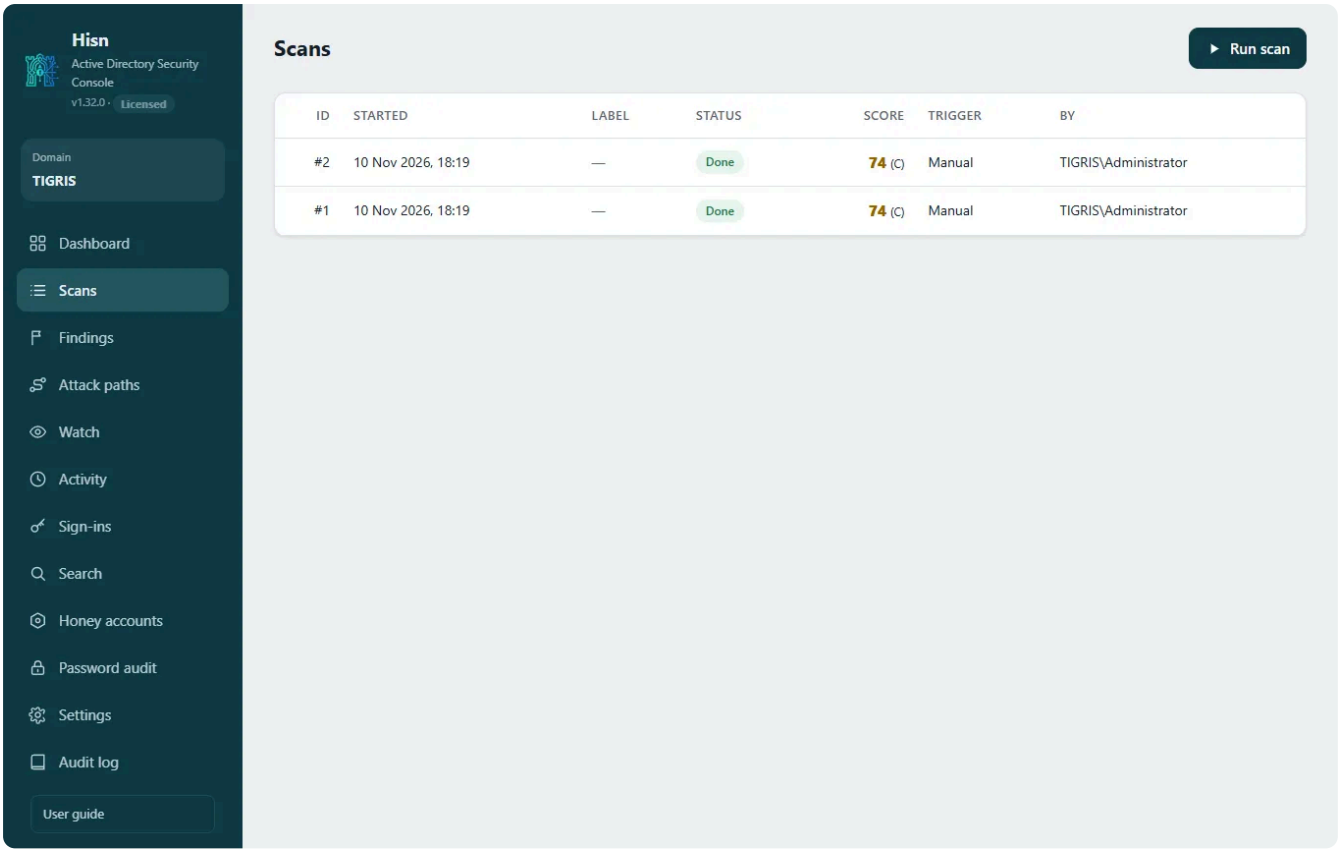
The lower half: top findings, attack paths, compliance coverage and Live Watch.

Lower down: the **top findings** (open the report from here), an **attack paths** summary, **compliance coverage** for each framework (click one for the Compliance page), and the **Live Watch** status with its interval, the changes it caught and the number of sources read without error.

---

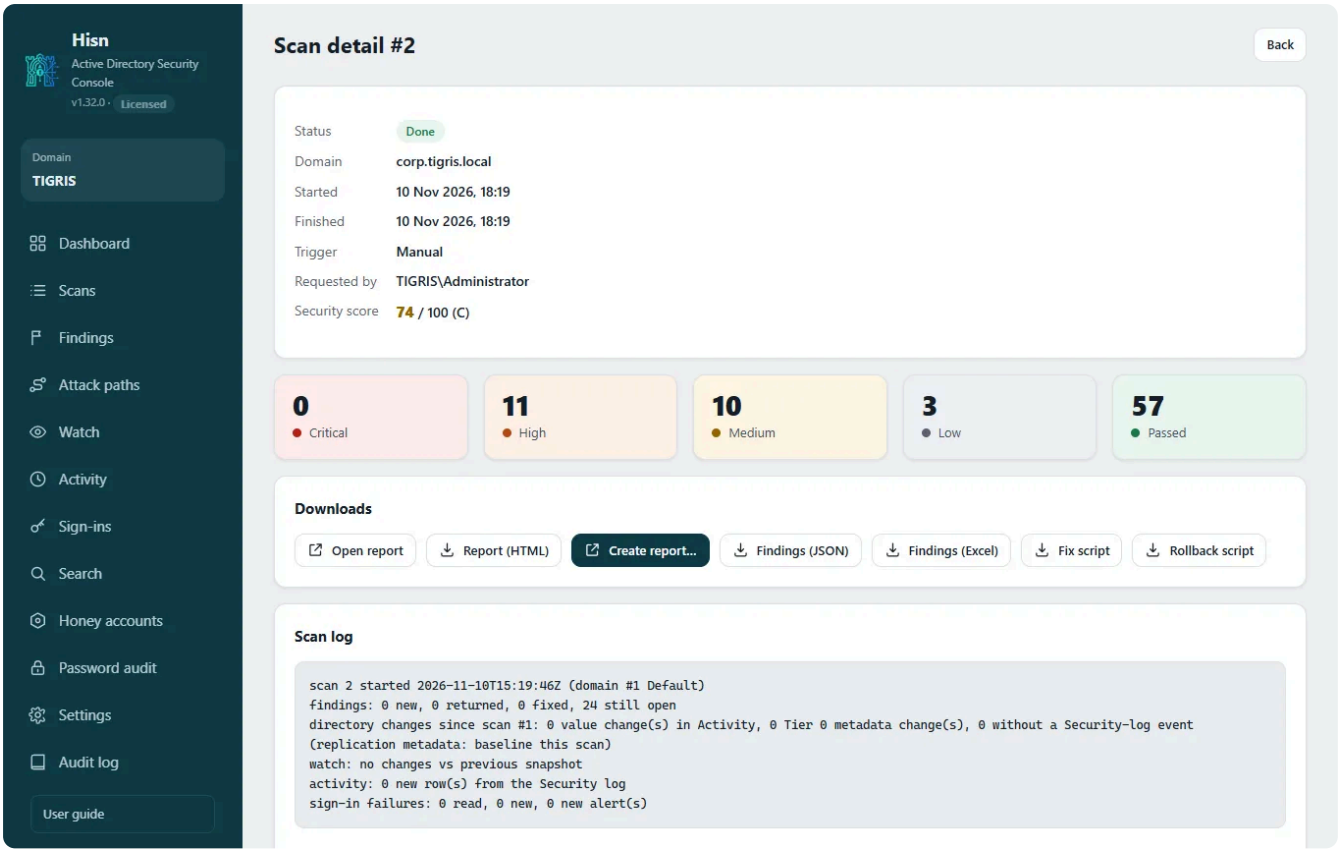
9. Scans and findings

Run a scan from *Scans* → *Run scan* or from the dashboard, or schedule it in *Settings* → *Scheduled scan* (daily or weekly; default Sunday 02:00). A medium domain takes 1 to 5 minutes; 20,000 accounts about 6 minutes (see Measured scan size).



Scans: every scan of the selected domain. Click one for its detail.

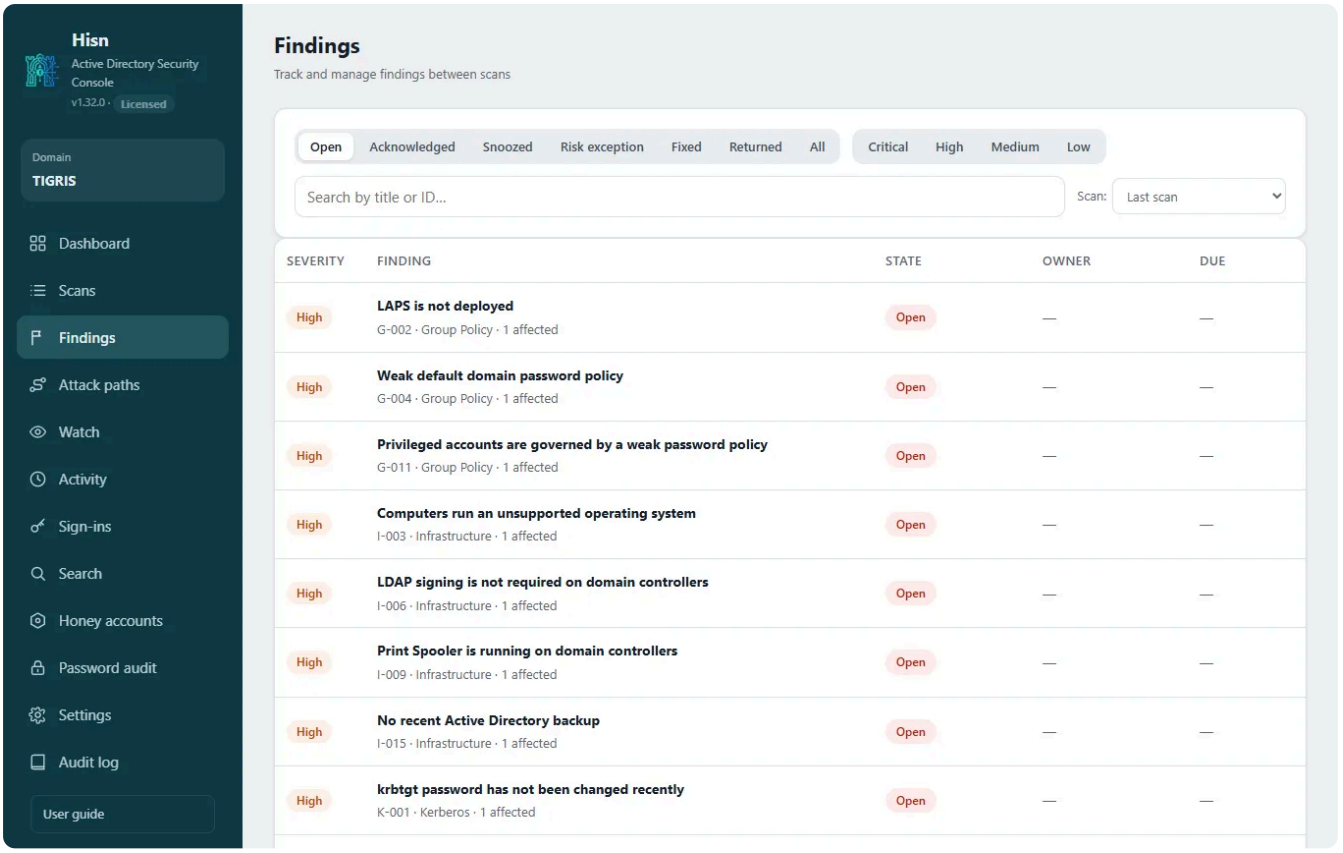
A scan's page shows its status, score and the count of findings by severity, the **downloads** (the report, findings as JSON or Excel, the fix and rollback scripts for every finding) and the scan log. **Create report…** opens the report builder (section 11).



A scan's detail, with its downloads and log.

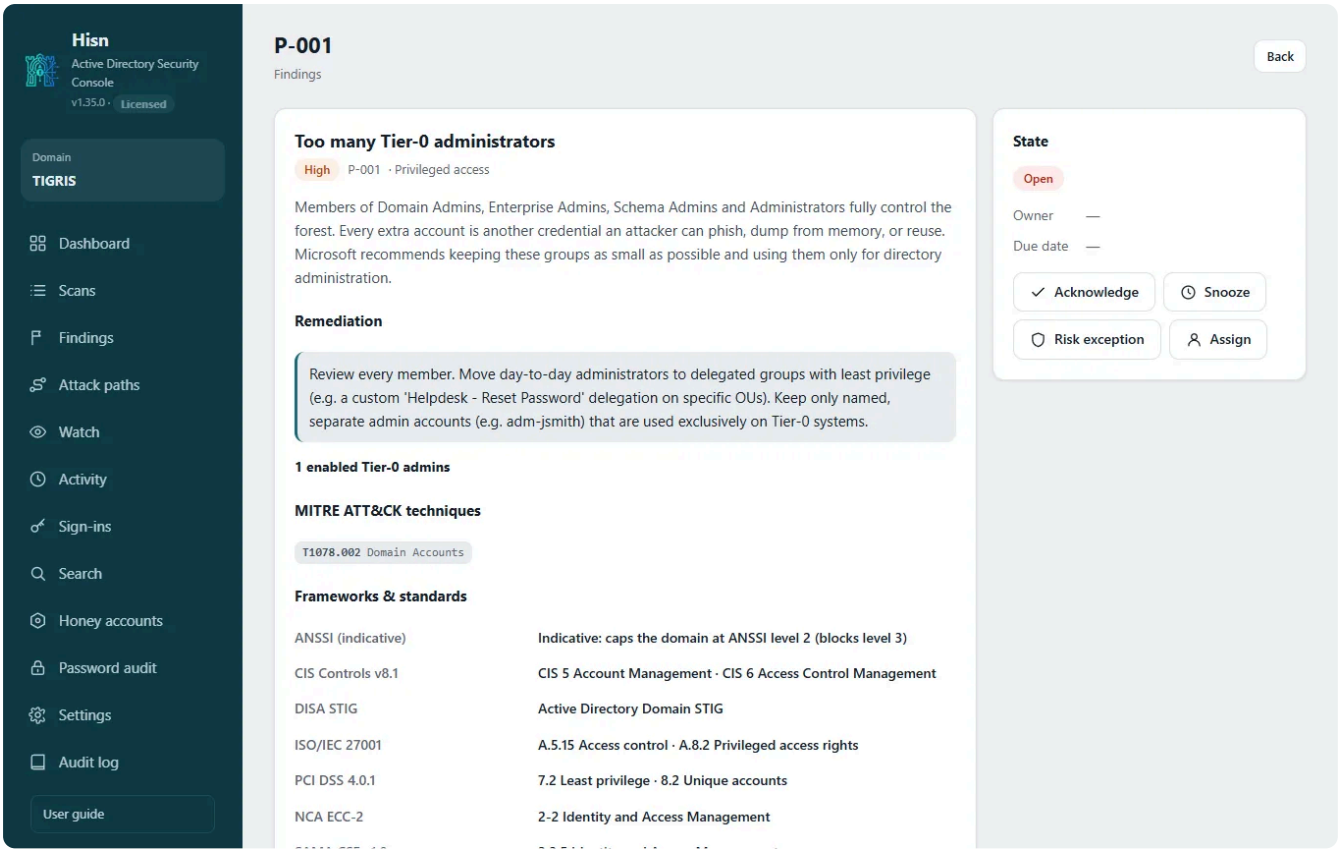
Findings

The *Findings* page lists what failed, filtered by state (open, acknowledged, snoozed, risk exception, fixed, returned) and severity, with a search by title or check ID. Each finding keeps its state across scans: when the next scan no longer sees the problem it becomes *fixed*, and if it comes back it is marked *returned*.



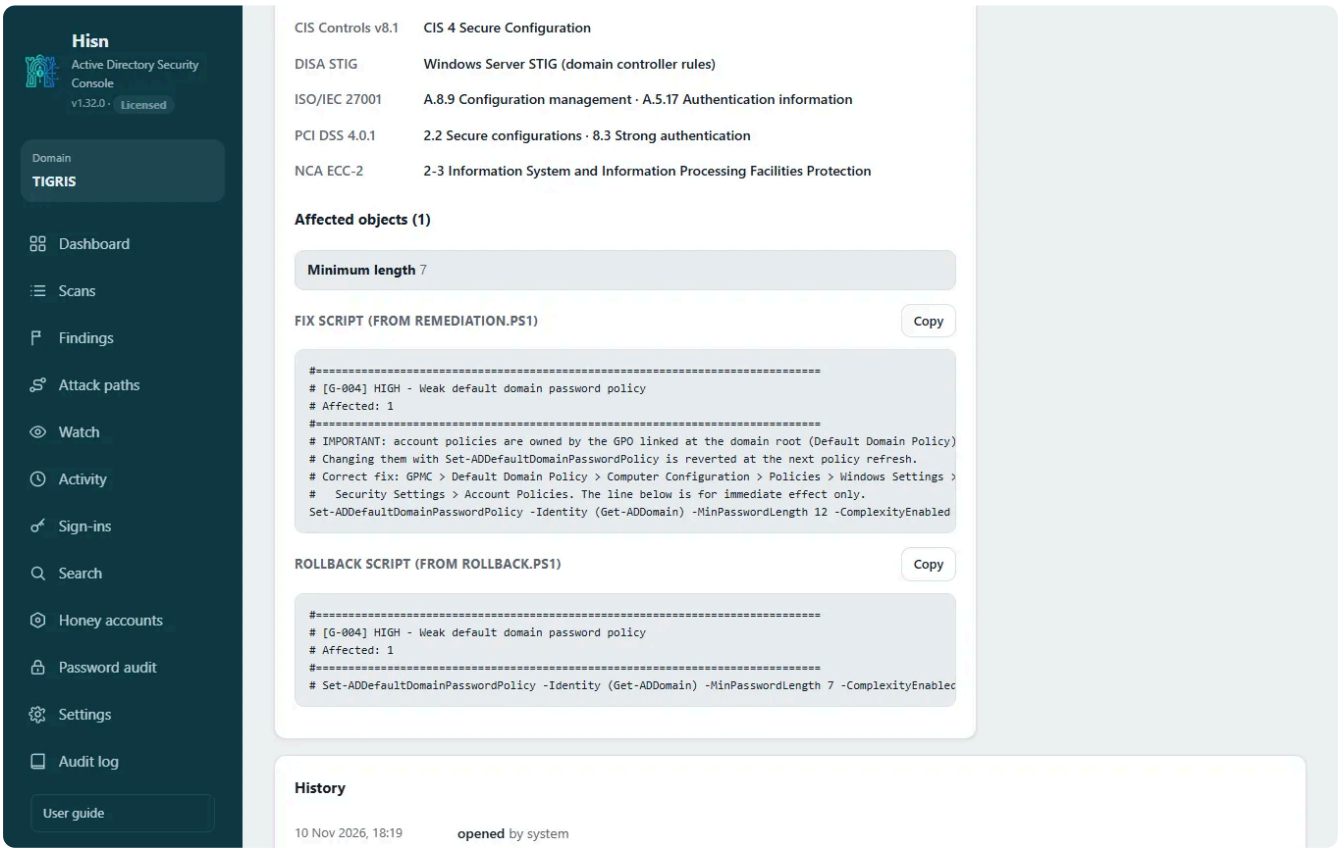
Findings, filtered to open ones.

A finding opens with an explanation, the remediation, the affected objects, MITRE ATT&CK techniques and the controls it maps to in each framework. On the right: **Acknowledge**, **Snooze** (up to 90 days), **Risk exception** (up to a year, with a reason) and **Assign** an owner and a due date. Every action is kept in the finding's history.



One finding: what it means, how to fix it, and where it maps.

Further down are the **fix script** and the **rollback script** for that finding. Read them, run the fix with `-WhatIf` first, and keep the rollback. Hisn never runs them itself.



Fix and rollback scripts, with comments that explain the correct fix.

- **Score.** Each area is weighted by severity (critical 10, high 5, medium 3, low 1). Any open critical finding holds the score at 59 (grade F): one critical path is enough to take over a domain.
- **Not evaluated** means the data could not be read (for example WinRM to a DC failed). The note under the check says why; it is never counted as passed.

---

10. Attack paths

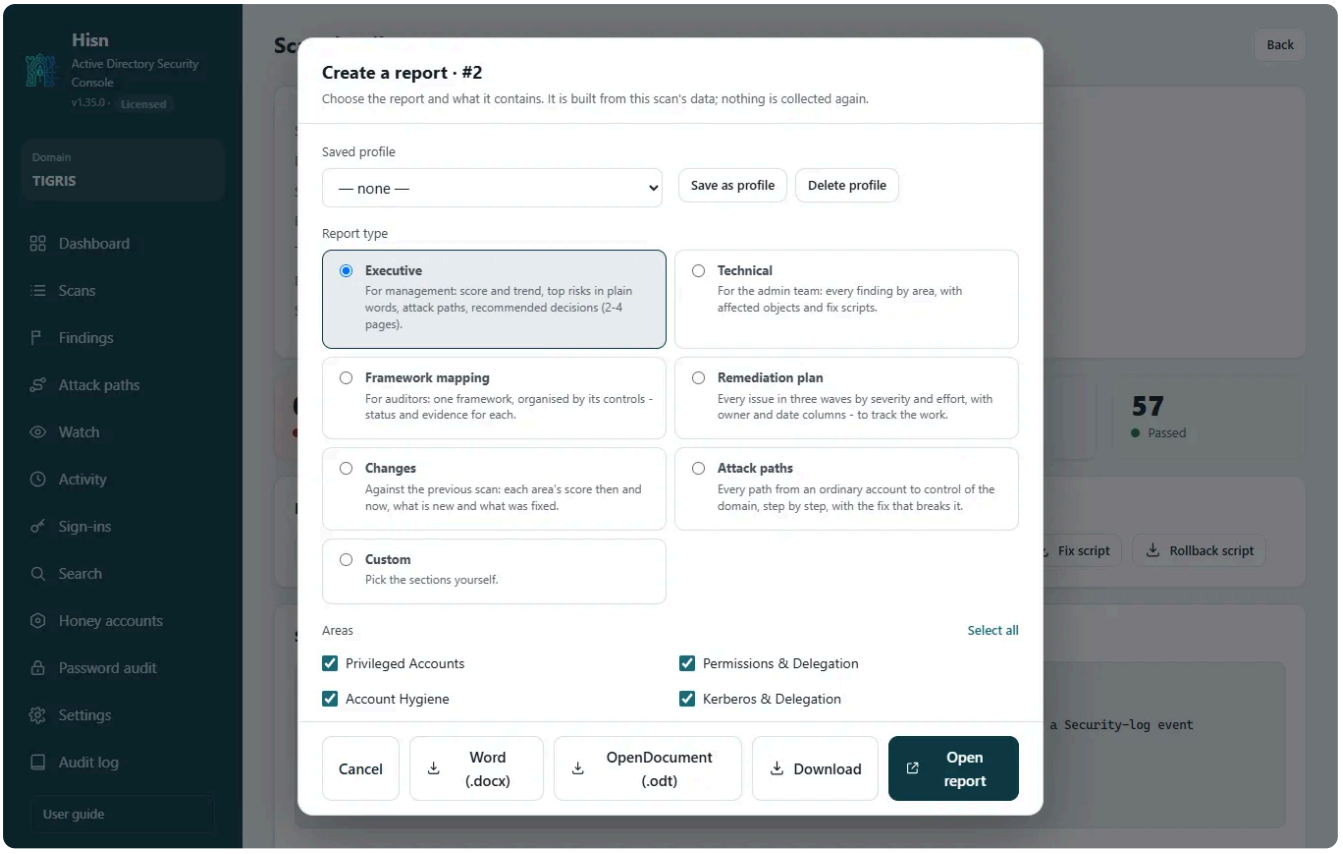
After each scan Hisn links permissions, group memberships, delegation, admin rights, sessions and certificate templates into a graph, and lists every chain from an ordinary account to full control of the domain (Tier 0). Each path names the single change that breaks it (*cut here*) with the PowerShell to make it; the top of the page shows the one change that closes the most paths (*best single fix*).

The tiles give the number of ordinary users with a path, the distinct paths, the shortest path in steps and the best single fix. "No attack paths" after a complete scan is the result to aim for. A note on the page says when the scan's permission data was incomplete; then scan again with the current version before relying on the result.

---

11. Reports

Open a scan and click **Create report…**. Every report is one HTML file that prints to A4 PDF, in Arabic or English, with a report ID and a SHA-256 fingerprint so a copy can be checked against the console. Reports are built from the scan's data; nothing is collected again.



The report builder: pick a type, the areas and options, then download or open the report.

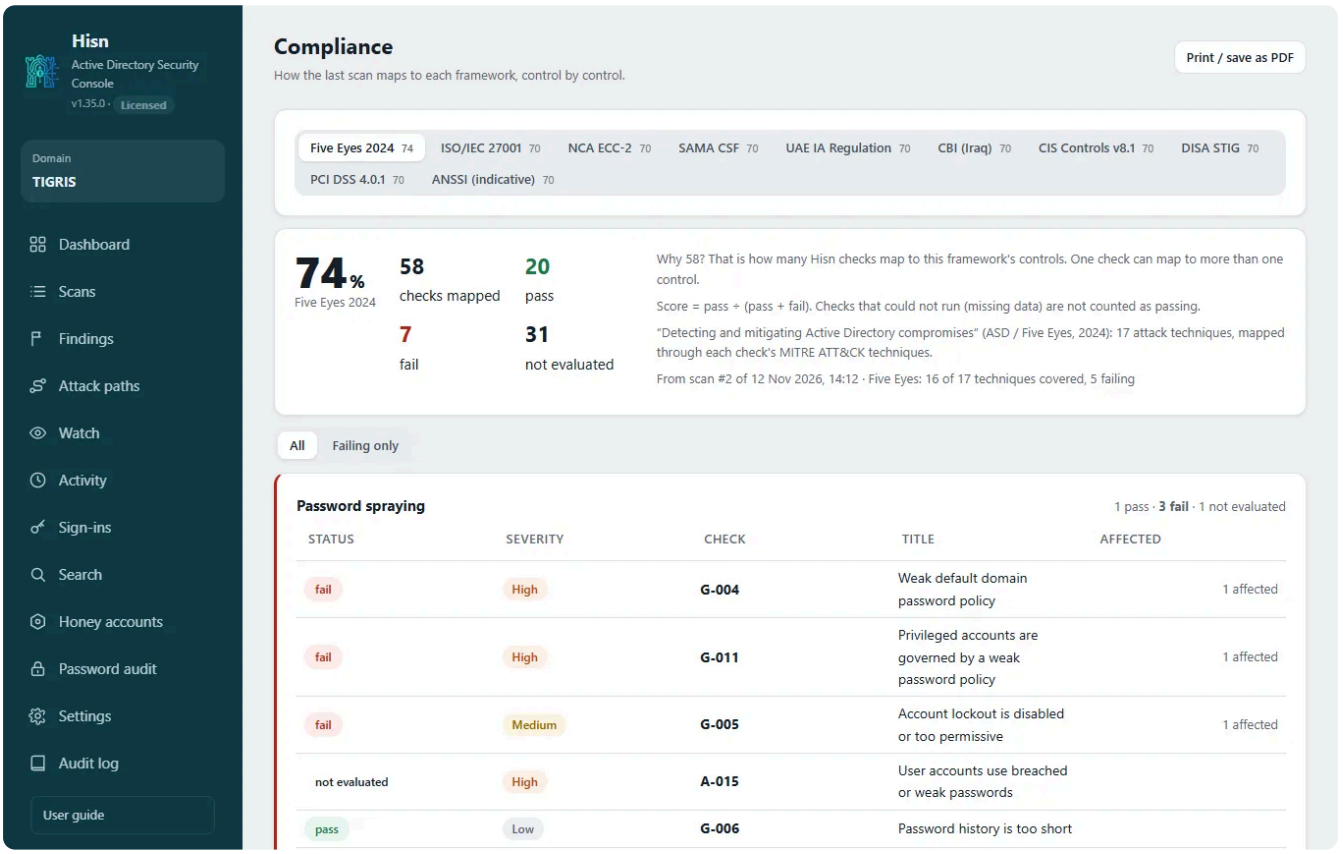
Type	For	Contents
Executive	Management	Score and trend, top risks in plain words, attack paths, recommended decisions (2 to 4 pages)
Technical	Administrators	Every finding by area, affected objects, fix scripts, ATT&CK coverage
Framework mapping	Auditors	One framework (ISO/IEC 27001, NCA ECC, SAMA CSF, UAE IA Regulation, Central Bank of Iraq cyber resilience controls, CIS Controls v8.1, PCI DSS 4.0.1, DISA STIG, ANSSI, Five Eyes) by its controls, with status and evidence
Remediation plan	Project tracking	Every issue in three waves by severity and effort, with owner, target date and done columns
Changes	Progress reviews	Each area's score then and now; new and fixed issues
Attack paths	Security team	Every path step by step, with the fix that breaks it
Custom	Anyone	Any of the 21 sections

Options: areas, severities, language, classification (None, Internal use, Confidential, Secret), fix scripts (admins only), passed checks, and theme (**Ishtar**, colourful; **Formal**, calm). Save a set of options as a **saved profile**; a profile can be e-mailed after every scheduled scan. Put your logo in *Settings → Organization logo*.

---

12. Compliance

Open *Compliance* from the dashboard's compliance card. It shows how the last scan maps to each framework, control by control. Hisn **maps** its checks to the frameworks; it does not certify compliance.

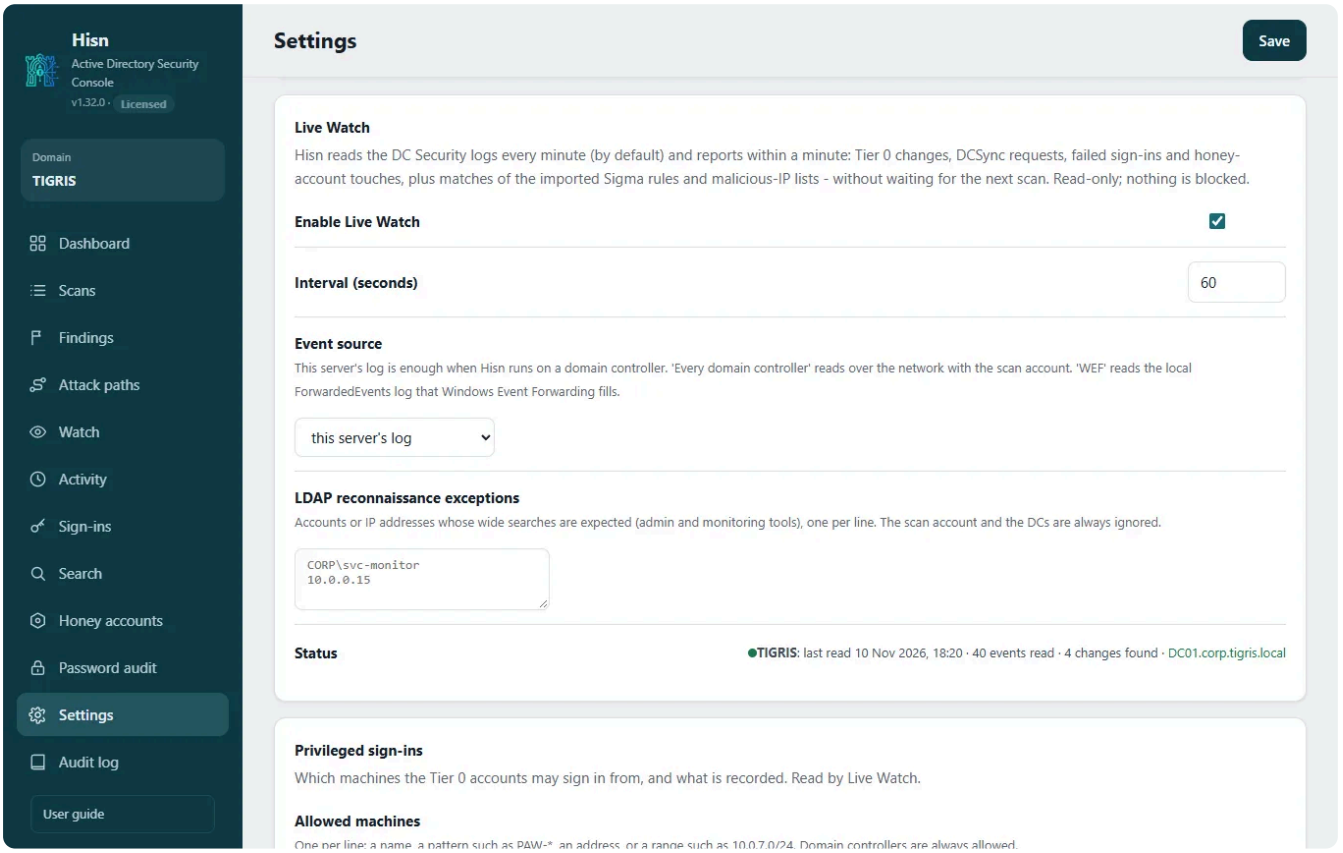


Compliance for one framework, with the checks under each control.

- The tabs at the top switch framework. The percentage is *pass ÷ (pass + fail)*; checks that could not run are shown as *not evaluated* and never counted as passing.
- One check can map to more than one control. *Failing only* hides the passing ones. **Print / save as PDF** prints the page.
- ANSSI is marked *indicative*: its levels are approximated from Hisn's checks.

13. Live Watch, Watch and Activity

Live Watch reads the DCs' Security logs every 15 to 900 seconds (default 60) and reports within about a minute: Tier 0 changes, DCSync, Kerberoasting and AS-REP roasting, LDAP reconnaissance, password spraying, brute force, lockout storms, user enumeration, honey-account use, Tier 0 sign-ins from machines outside Tier 0, Sigma rule matches and sign-ins from addresses on imported threat lists. Several domains are read at the same time, and a window that could not be read is read again later. Turn it on in *Settings → Live Watch*.



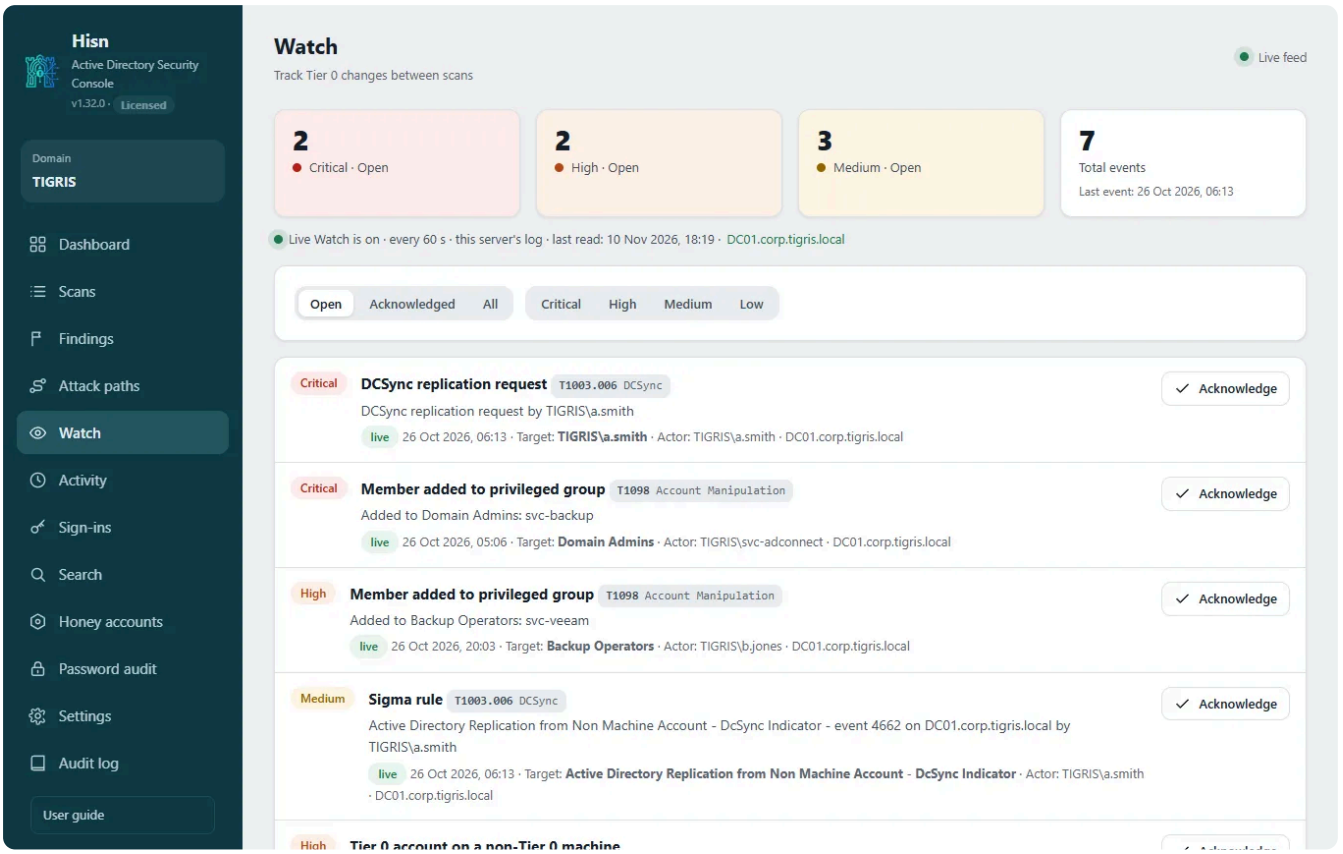
Settings → Live Watch, with its status line at the bottom.

Event source: this server's own log (Hisn on a DC), every DC over the network, or the ForwardedEvents log when Windows Event Forwarding sends DC logs here.

> **Audit policy needed on the DCs** (Default Domain Controllers Policy → Advanced Audit Policy Configuration, Success and Failure): Kerberos Authentication Service, Kerberos Service Ticket Operations, Credential Validation, Logon, User Account Management, Security Group Management, Computer Account Management, Directory Service Changes, Directory Service Access. Check M-001 tells you which are missing.

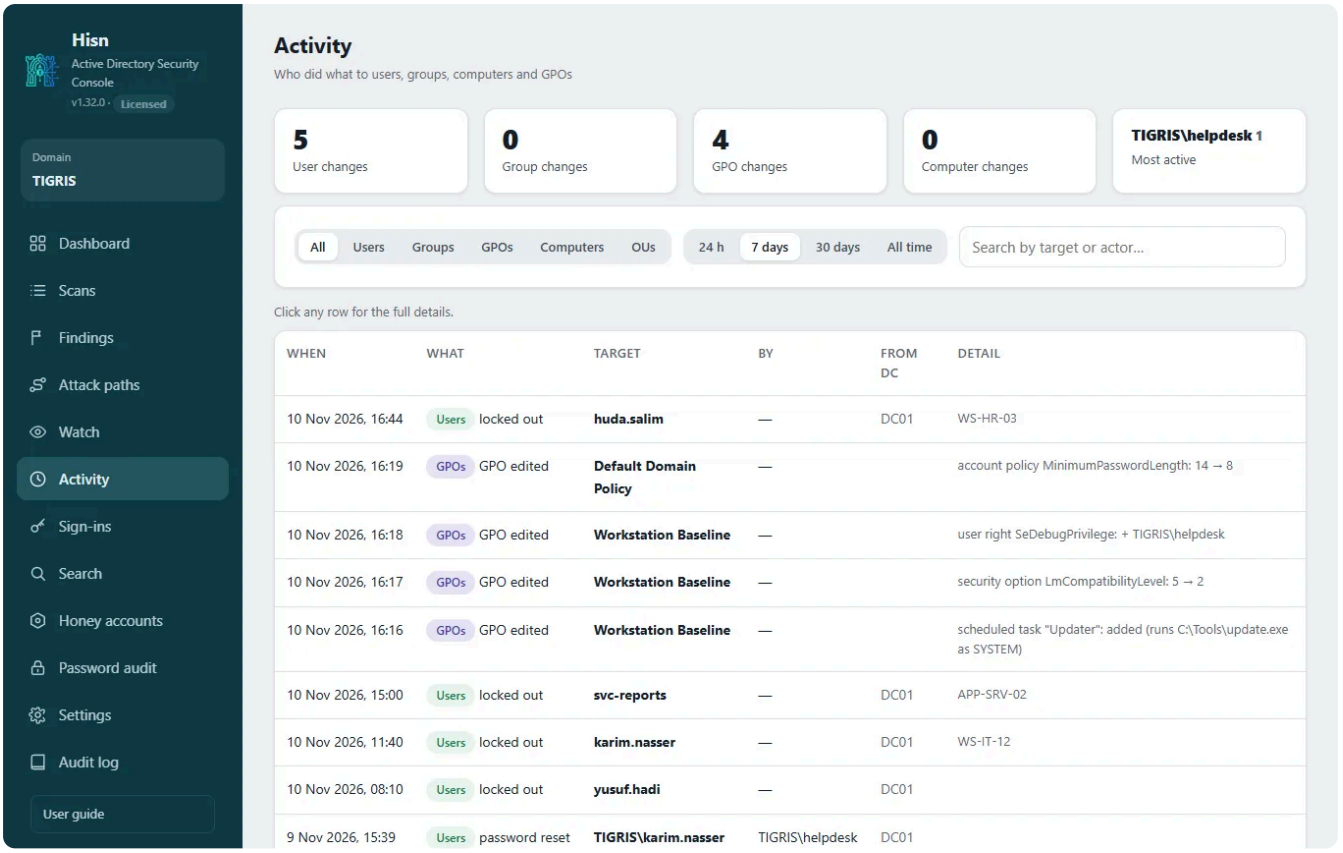
Watch lists every change and alert, from Live Watch and from comparing each scan with the previous one: privileged groups, AdminSDHolder, domain-root permissions, DC GPOs,

certificate templates, trusts, krbtgt, DCs and FSMO roles. Each entry has a severity, its MITRE ATT&CK technique, the target, the actor and the DC. A change found by a scan with no matching Security-log event is flagged as a *silent change* (made while auditing was off, or the log was cleared). Review an entry and press **Acknowledge**.



Watch: alerts and Tier 0 changes waiting for review.

Activity answers "who did what": user, group, computer, GPO and OU changes from the Security log and from scan comparisons, with the actor and the DC. For GPOs it says which setting changed (section 14). Filter by kind and time, search by target or actor, and click a row for the full details.

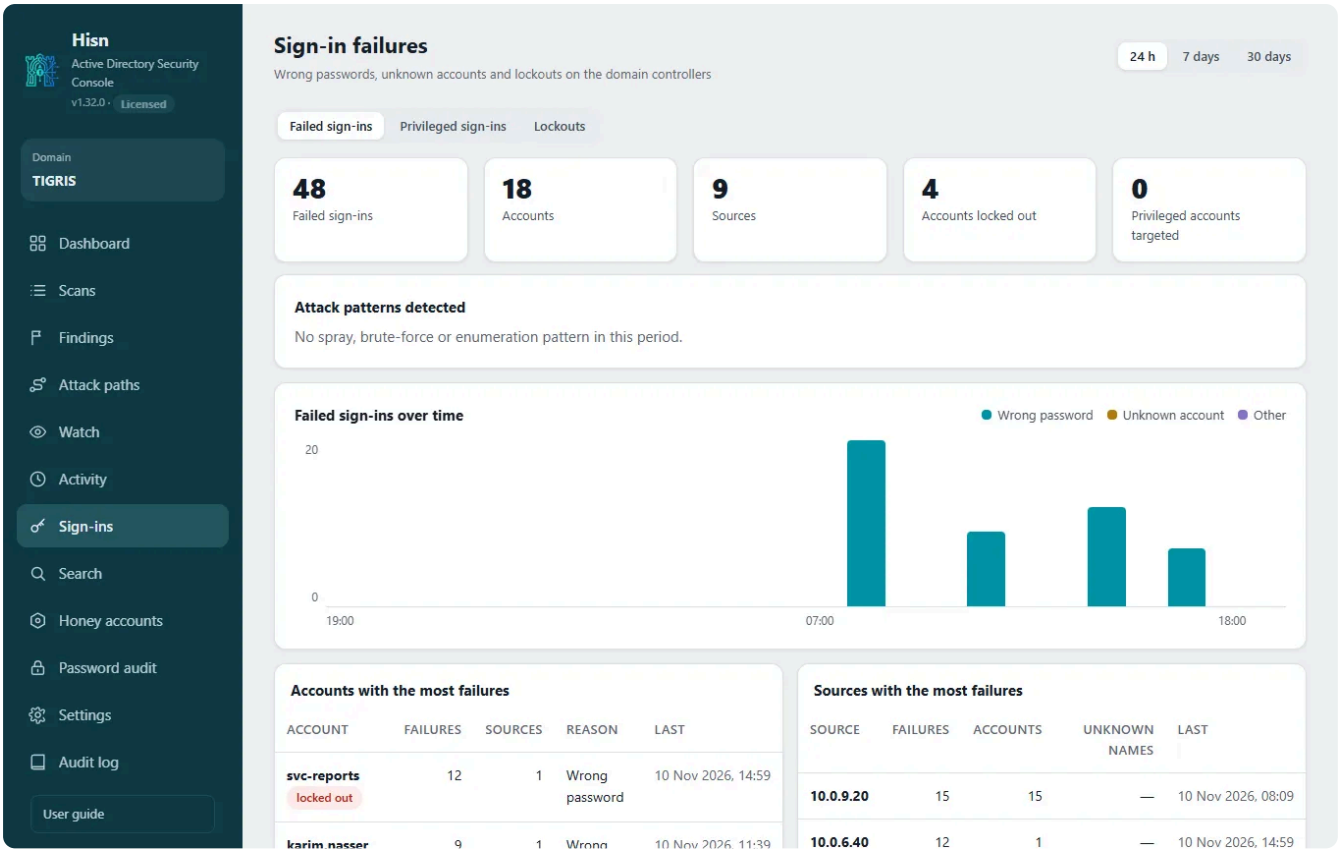


Activity, including Group Policy setting changes.

14. Sign-ins, lockouts and search

The *Sign-ins* menu has three tabs: **Failed sign-ins**, **Privileged sign-ins** and **Lockouts**. All of them read what Live Watch and the scans have recorded; nothing is changed in Active Directory.

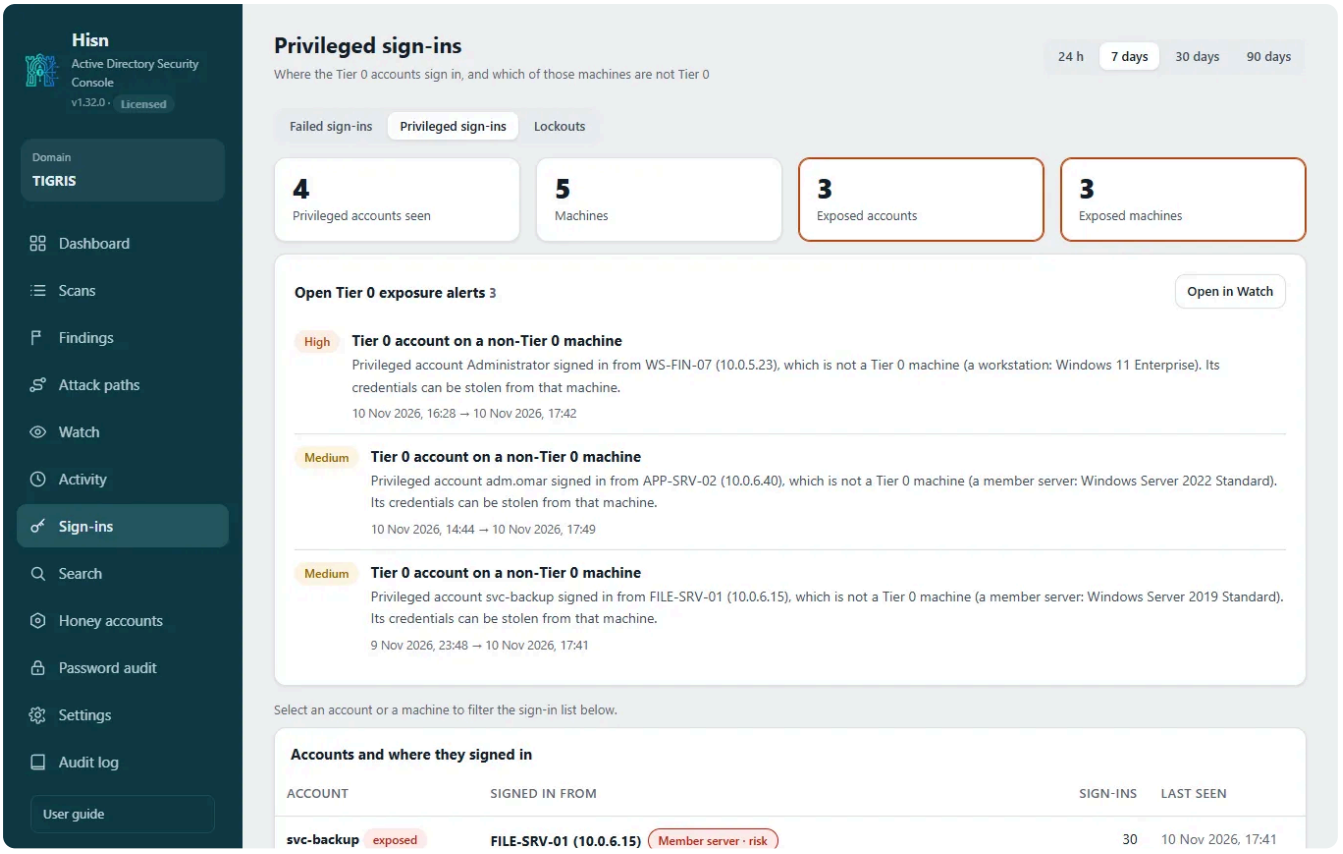
Failed sign-ins shows wrong passwords and unknown account names by account and by source, over 24 hours, 7 or 30 days, and the alerts raised from them (password spraying, user enumeration, brute force, failures on privileged accounts, lockout storms).



Failed sign-ins over time, by account and by source.

Privileged sign-ins

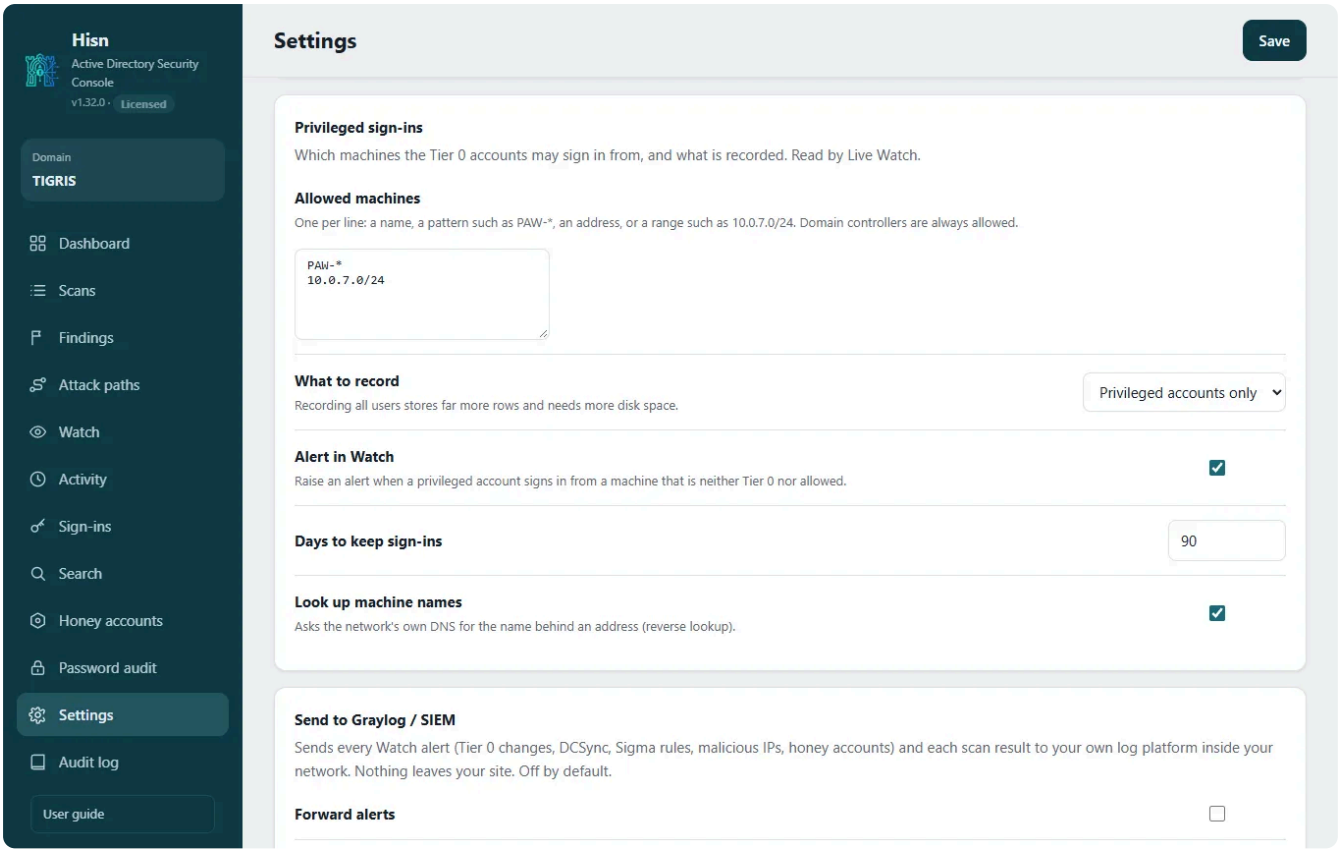
A privileged account leaves its password hash or Kerberos ticket on every machine it signs in to, and whoever controls that machine can take them. With Live Watch on, Hisn records the successful sign-ins of the Tier 0 accounts (Kerberos ticket requests, event 4768, and logons at a domain controller, event 4624) and shows which account signed in from which machine.



Privileged sign-ins: three Tier 0 accounts were used on machines outside Tier 0.

- **Tier 0** (a domain controller) and **Allowed** (a machine on your allowed list) are fine.
- **Workstation**, **Member server** and **Unknown machine**: the account's credentials are exposed there. Hisn raises the alert *Tier 0 account on a non-Tier 0 machine*, high for a workstation and medium otherwise, once per account and machine per week.
- Below the alerts, select an account or a machine to filter the list of sign-ins.

What to do: administer the domain only from dedicated admin workstations or jump servers, and list them in *Settings → Privileged sign-ins → Allowed machines*, one per line: a name (`PAW-01`), a pattern (`PAW-*`), an address, or a range (`10.0.7.0/24`). An entry Hisn cannot use is refused with a message. A service account that is a member of a Tier 0 group and runs on a member server is reported too; that is a real exposure, so take it out of the group rather than allowing the server.



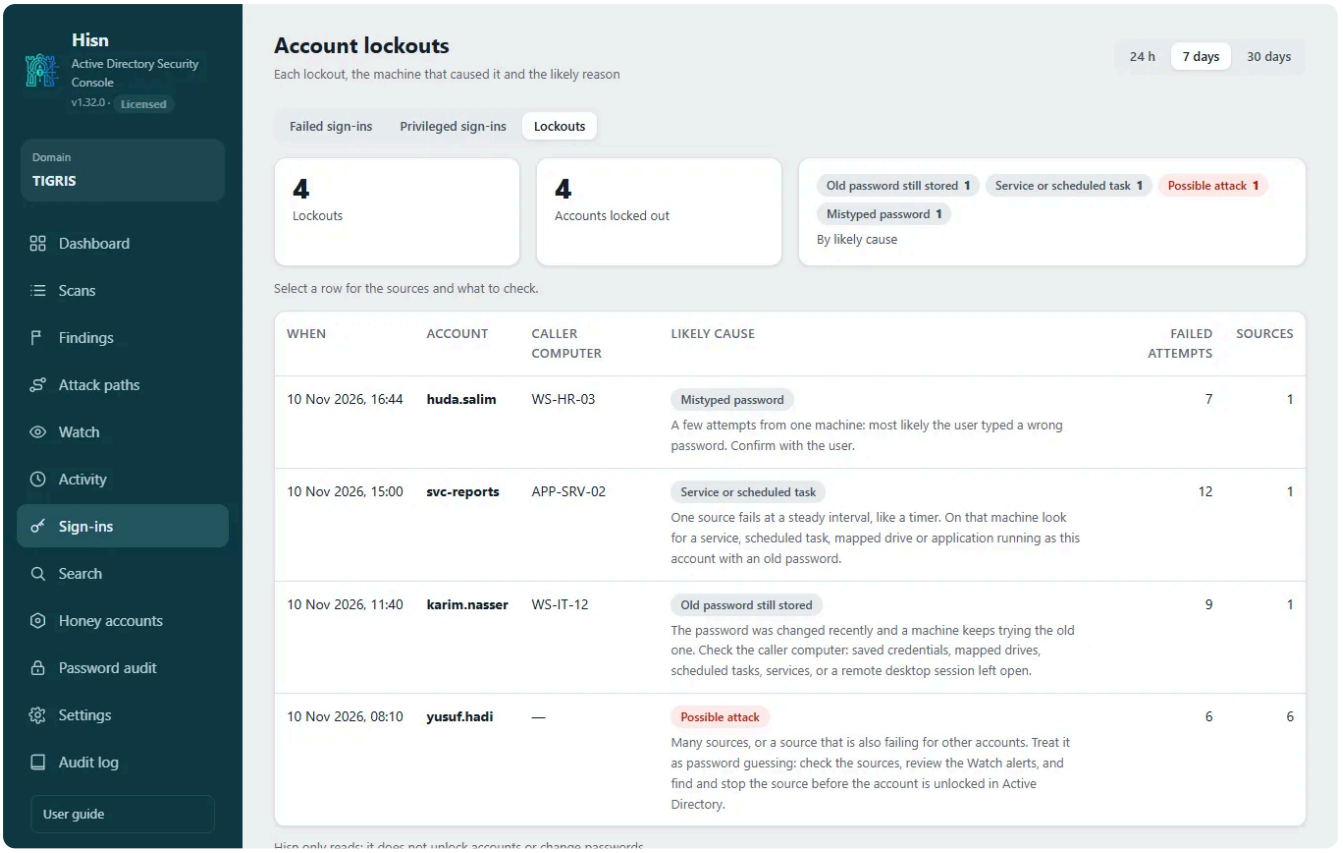
Settings → Privileged sign-ins.

Machine names come from the event itself or from a reverse DNS lookup made from the Hisn server inside your network; the lookup can be switched off. By default only privileged accounts are recorded, and sign-ins are kept 90 days. Recording *all users* keeps every user's ticket requests as well; on a large domain that is many rows, so choose it only if you need sign-in history for everyone.

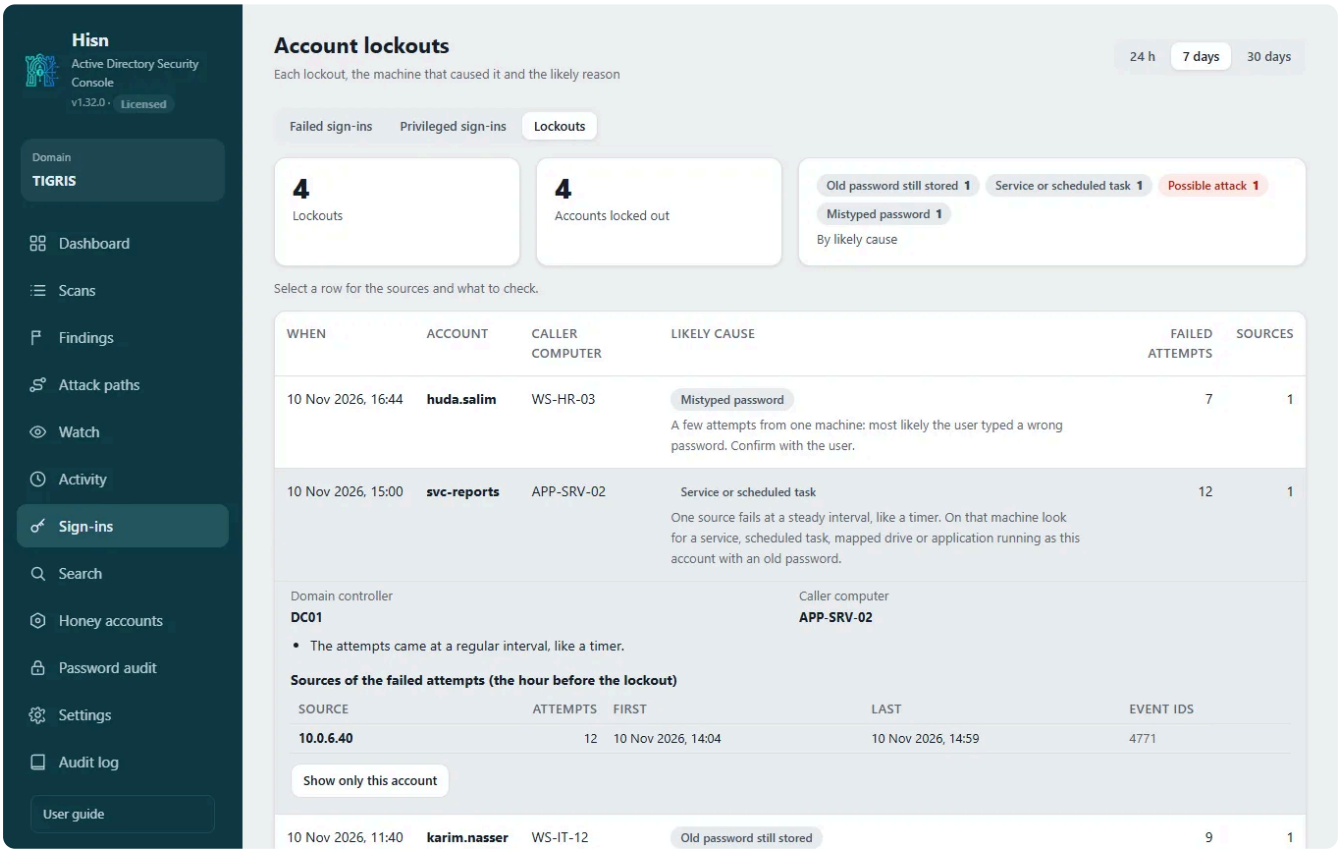
> **Audit policy needed on the DCs:** Kerberos Authentication Service (Success) and Logon (Success). Both are on by default on domain controllers.

Lockouts

Each account lockout is shown with the machine that caused it (the caller computer of event 4740), the failed attempts in the hour before it, and the likely cause. Select a row for the sources and what to check.



Lockouts, each with its likely cause and what it means.



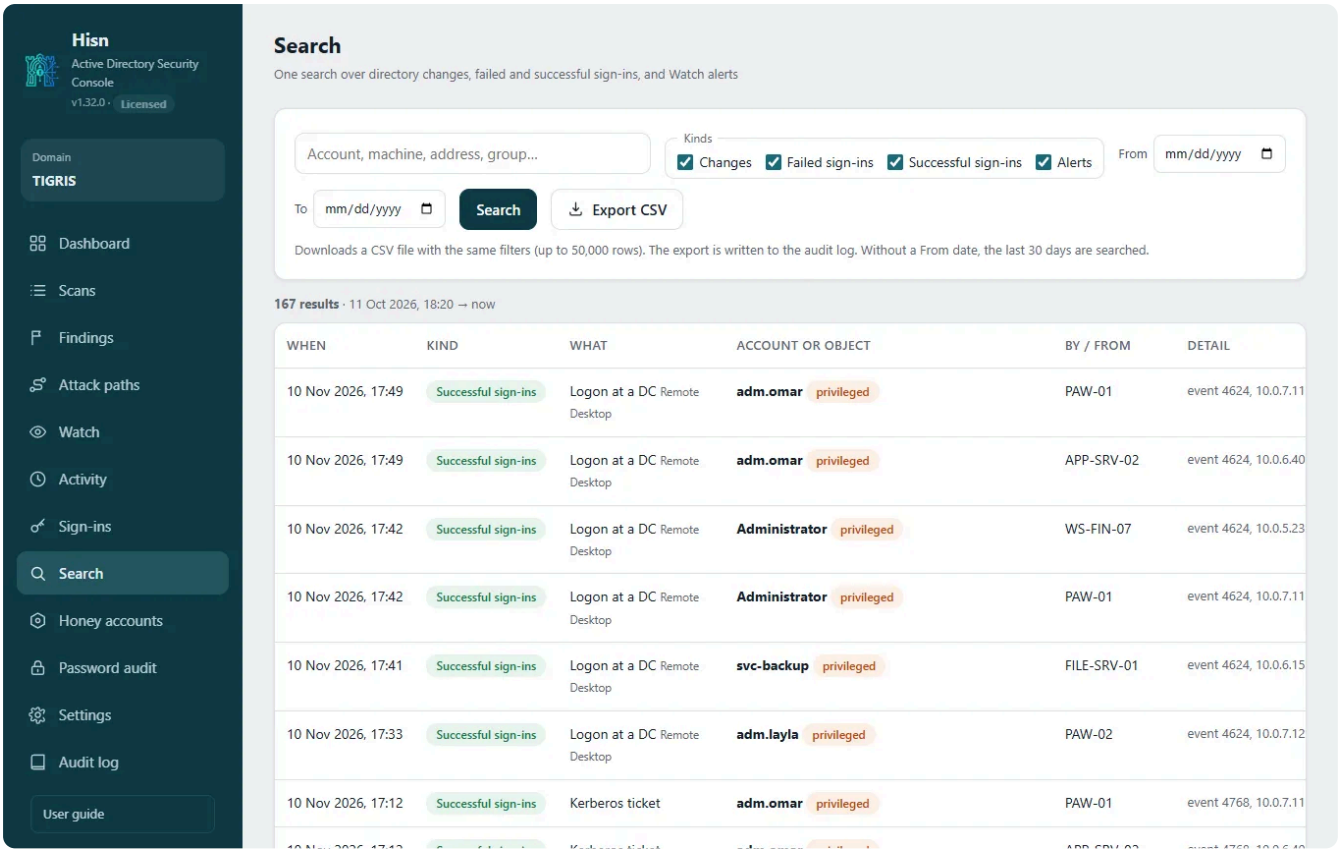
One lockout opened: the attempts came at a regular interval, so a service or task is the likely cause.

Likely cause	What it means	What to check
Old password still stored	The password was changed in the last 7 days and one or two machines keep trying the old one	Saved credentials, mapped drives and mail profiles on the machines listed
Service or scheduled task	One source failing at a steady interval	Services, scheduled tasks and application pools running as that account on the source
Phone or other device	NTLM attempts from one named device, again and again	The phone, mail client or Wi-Fi profile of the user
Possible attack	Many sources, or a source that is also failing for other accounts	The Failed sign-ins tab and the Watch alerts for the same time
Mistyped password	A few attempts from one machine	Confirm with the user
Cause unknown	No failed sign-in was recorded before the lockout	The audit policy on the DCs (check M-001)

Hisn does not unlock accounts. The cause is an estimate from the recorded events, not a verdict.

Search

Search looks through everything Hisn has recorded for the domain in one list: directory changes (Activity), failed sign-ins, successful sign-ins and Watch alerts. Filter by text (an account, machine, address or group), kind and date; without a start date the last 30 days are searched. **Export CSV** downloads the result with the same filters (up to 50,000 rows) for an auditor; the export itself is written to the Audit log. The page states how long each kind is kept; change that in *Settings*.



Search across changes, failed and successful sign-ins and alerts.

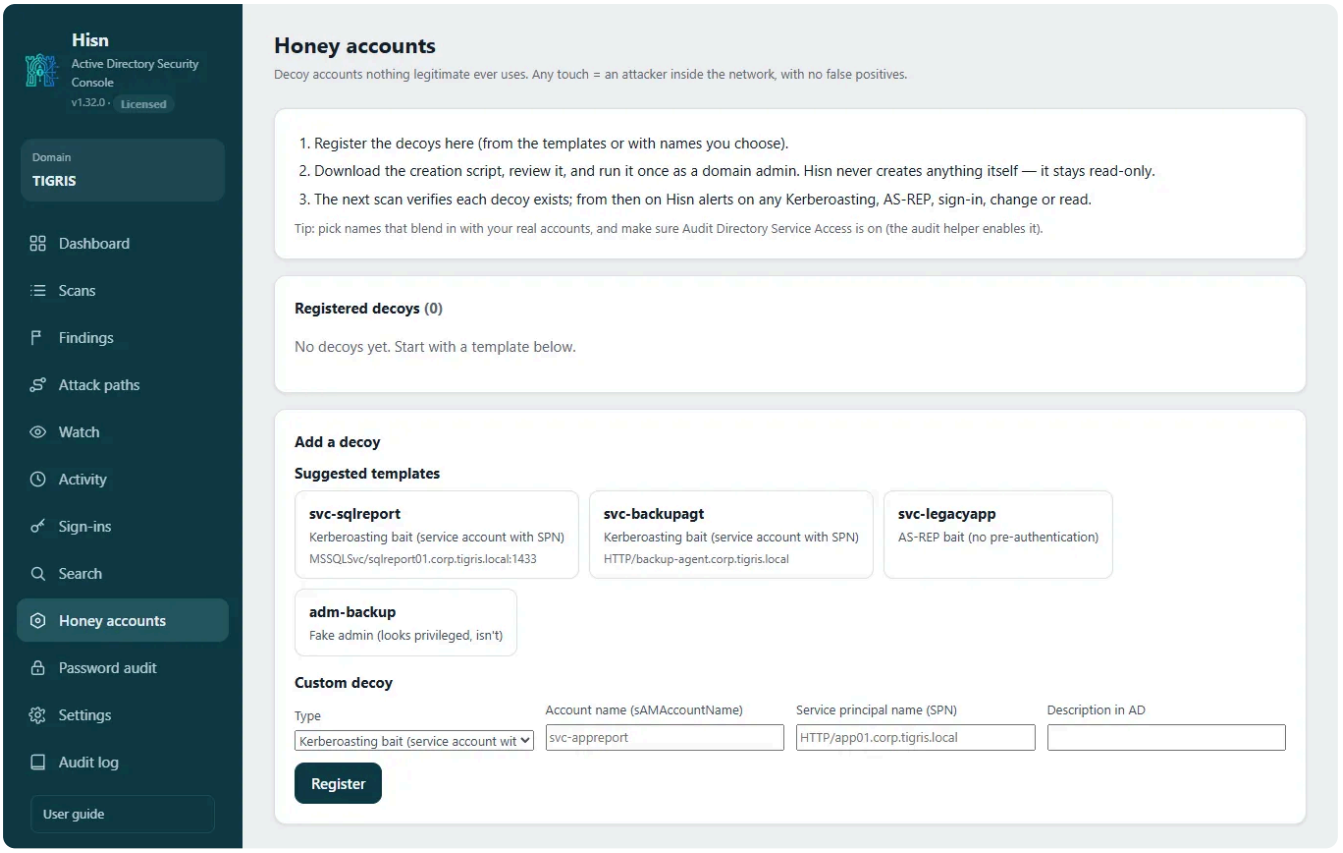
Which Group Policy setting changed

From collector 1.3.0, *Activity* shows which setting changed inside a GPO between two scans, with the old and the new value: user rights, security options, password, lockout and Kerberos policy, registry settings, restricted groups, scheduled tasks and scripts (see the Activity picture in section 13). The first scan after the upgrade records the starting point; details appear from the second scan. Windows service and IIS application pool identities in user rights are labelled as such, because their names cannot be read back from their SIDs. Password values stored in a GPO are never collected.

---

15. Honey accounts

Honey accounts are decoys that nothing legitimate ever uses, so any touch means someone inside the network is looking for a way in. Hisn suggests decoys that attract common attacks (a service account with an SPN for Kerberoasting, an account without Kerberos pre-authentication for AS-REP roasting, a fake administrator) or takes names you choose.



Honey accounts: register, create with the script, and the next scan verifies them.

1. Register the decoys on this page (from the templates or with your own names that blend in).
2. Download the creation script, review it, and run it once as a domain admin. Hisn never creates anything itself.
3. The next scan verifies that each decoy exists. From then on Hisn alerts on any Kerberoasting, AS-REP request, sign-in, change or read of a decoy. Reads need *Audit Directory Service Access* on the DCs.

---

16. LDAP reconnaissance sensor

To see BloodHound-style enumeration, each DC must log LDAP searches (event 1644). Run the script once on every DC, from `C:\Program Files\Hisn\collector` (copy it to DCs where Hisn is not installed):

```
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1 -WhatIf   #
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1           #
powershell -ExecutionPolicy Bypass -File .\Enable-HisnLdapSensor.ps1 -Status   #
```

It saves the previous values, and `-Disable` restores them. Accounts and addresses that legitimately enumerate AD (inventory tools, Hisn itself) can be listed under *Settings → Live Watch → LDAP reconnaissance exceptions*.

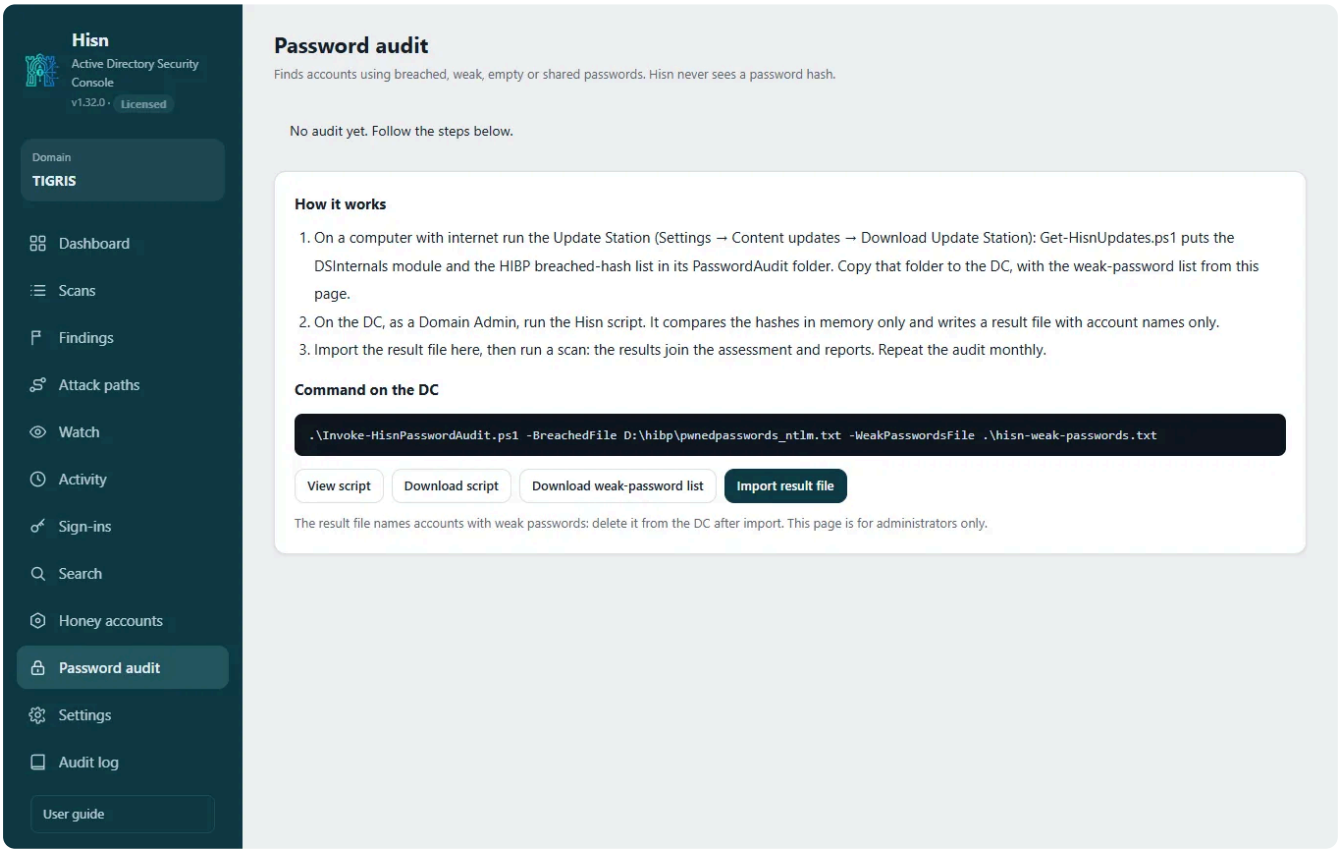
---

17. Password audit

Finds breached, weak, empty, shared and LM-stored passwords (checks A-014 to A-018). Run it yourself as a Domain Admin on a DC; it uses the free DSInternals module and keeps hashes in memory only.

```
Install-Module DSInternals
.\Invoke-HisnPasswordAudit.ps1 -BreachedFile D:\hibp\pwnedpasswords_ntlm.txt -We
```

Import the resulting `.json` on the *Password audit* page. It contains account names only and is used by scans for 90 days. The page also offers the script and a weak-password list to download.



Password audit: run it on a DC, then import the result here.

18. Content updates (offline)

Detection rules and intelligence (Microsoft security updates by build, CISA KEV, EPSS, Windows support end dates, Sigma rules, malicious IP lists, weak-password lists) arrive as signed `.hcb` packages. Import them in *Settings → Content updates*; tampered or unsigned files are refused. On an internet-connected PC, the **update station** (downloadable from the same page) fetches new packages for you to carry in. The server never sends anything out.

19. E-mail and SIEM

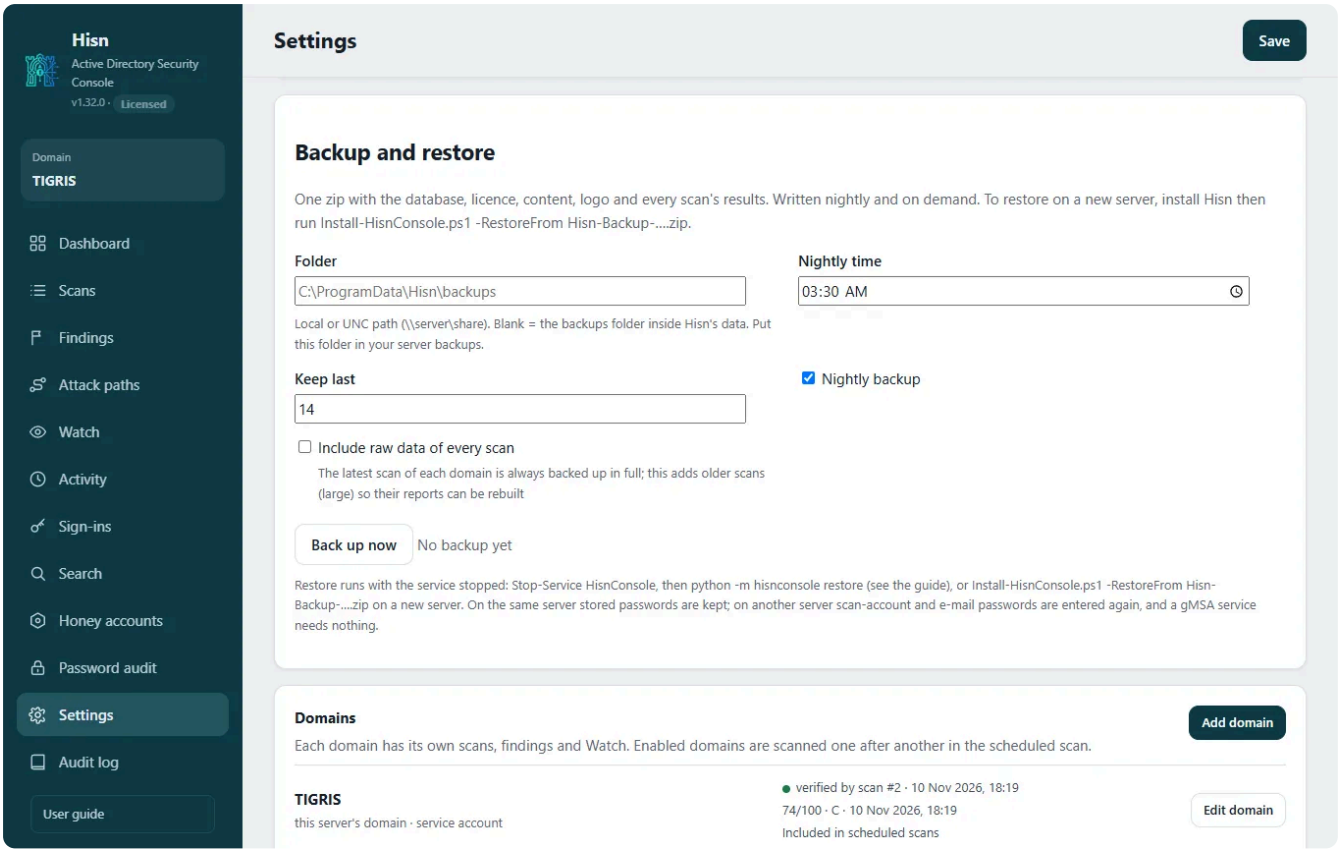
E-mail (*Settings → Email (SMTP)* and *Watch alerts*): SMTP server, port, encryption and sender; send the scan report (choose a saved profile) after scheduled scans, and Watch alerts above a minimum severity. Alerts are sent in the background, and several alerts for the same domain within a few seconds arrive as one message, in English and Arabic.

SIEM (*Settings → Send to Graylog / SIEM*): forwards alerts and audit events to Graylog or any syslog receiver as GELF, CEF or JSON, over UDP, TCP or TLS. Off by default.

20. Data, backup and restore

Location	Contents
`C:\Program Files\Hisn`	Program, collector scripts, embedded Python (replaced on upgrade)
`C:\ProgramData\Hisn`	Database, scan folders, licence, content, logo, certificate, logs, backups (kept on upgrade; SYSTEM and Administrators only)

Backup



Settings → Backup and restore.

Every night at the set time (default 03:30) the console writes one file, `Hisn-Backup-<server>-<date>.zip`, and keeps the newest *N* (default 14). **Back up now** writes one on demand. The zip holds the database (a consistent copy, safe while the service runs), `config.json`, the licence, content packages, the logo and every scan's results and reports. The raw collection data of each domain's latest scan is always included, because the domain ID, dashboard counts, report rebuilds and the next scan's comparison read it. Older scans' raw data is added only if you tick *Include raw data of every scan*.

Set the folder to a path your server backup already covers; a UNC share such as `\\backup01\hisn` works, and the service account needs write access to it. Blank means `C:\ProgramData\Hisn\backups` on the console itself, which protects against a bad upgrade but not against losing the server.

From the command line (for scripts and scheduled jobs): `"C:\Program Files\Hisn\python\python.exe" -m hisnconsole backup --data C:\ProgramData\Hisn --to D:\Backups\Hisn`, with `PYTHONPATH` set to `C:\Program Files\Hisn\console;C:\Program Files\Hisn\engine`.

Restore

- **On the same server, from the console:** in *Settings → Backup and restore*, click **Restore** next to a backup and type `RESTORE`. Hisn restarts, saves a safety copy of the current state, restores the backup and comes back on its own; sign in again when the page reloads. If anything fails it returns to the safety copy and Settings says why. Everything newer than the backup is replaced.
- **On a new server:** run Setup and choose the backup on its *Restore from backup* page, or `Install-HisnConsole.ps1 -RestoreFrom <zip>`. The installer restores before the service starts.
- **From the command line:** `"C:\Program Files\Hisn\HisnConsole.exe" stop`, then `python.exe -m hisnconsole restore --data C:\ProgramData\Hisn --from <zip>` (same `PYTHONPATH` as above), then `HisnConsole.exe start`. The previous database is kept as `hisn.db.pre-restore`.

After a restore on another server, a notice in Settings says which stored passwords were cleared: scan-account, SMTP and SIEM passwords are protected for the old server (Windows DPAPI) and cannot move. Enter them again, then dismiss the notice. A service running as a **gMSA** needs nothing. The licence travels with the backup, because it is bound to your domain IDs. A backup from an older Hisn is upgraded on the first start (with its own `hisn.db.bak-*` copy); a backup from a *newer* Hisn is refused: install that version first.

Not in the backup: the server's TLS certificate (a new one is generated), logs, and `config.json` on restore unless `--with-config` is given. Measured in the lab (3 domains, 15 scans, 2.6 MB backup): stop, restore, start and sign in took about one minute.

Uninstall: Settings → Apps → *Hisn AD Security Console*. You are asked whether to keep the data for a later reinstall.

21. Troubleshooting

Symptom	Cause and fix
Blank page or "needs Edge, Chrome or Firefox"	Internet Explorer. Open the address in Edge, Chrome or Firefox.
WinRM error `0x80090322`	Kerberos reached the wrong account. Either the DC's name resolves to another machine's address (a second network card registered in DNS: remove those records, or add the right address to the hosts file), or the name `HTTP/<server>` is registered on another account. Hisn retries with the port in the name; register it once on the server: `setspn -S HTTP/<fqdn>:5985 <SERVER>` and `setspn -S HTTP/<short>:5985 <SERVER>`. Test connection names the account that holds the name.
WinRM "Cannot find the computer" (Kerberos)	Usually the same cause: a gMSA or service account holds `HTTP/<server>`. Register the port-specific names as above.
Member server "access denied"	The scan account (or `DOMAIN\DC$`) is not in the server's local Administrators.
Many checks "not evaluated" for one domain	WinRM to its DC failed; run Test connection and fix the reported cause, then scan again.
A scan or backup does not start: "low disk space"	Free space is below the minimum (2 GB by default). Free some space, or lower the minimum in Settings.
Privileged sign-ins page is empty	Live Watch is off, or no scan has listed the Tier 0 accounts yet. Turn on Live Watch and run a scan.
Script blocked by execution policy	Run collector scripts with `powershell -ExecutionPolicy Bypass -File <script>`; this applies to that one command only.

Console does not open	`Get-Service HisnConsole` ; logs in `C:\ProgramData\Hisn\logs\console.log` and `C:\ProgramData\Hisn\logs\HisnConsole.err.log` ; Start → Hisn → *Hisn health check*.
"This database is from a newer Hisn"	An older version was installed over a newer database. Install the newer version again, or restore a backup made with this version.
Port 8443 already in use	Run Setup again and choose another port.

---

22. Glossary

Tier 0
The accounts, groups and machines that control the whole domain: domain controllers, Domain Admins, Enterprise Admins and the like. Whoever controls one of them controls everything.

Finding
A check that failed in a scan, with the objects affected. It keeps a state (open, acknowledged, snoozed, risk exception, fixed, returned) across scans.

Attack path
A chain of permissions, memberships or sessions that lets an ordinary account reach Tier 0.

Exposure
A privileged account's credentials left on a machine outside Tier 0, where they can be stolen.

Allowed machine
An admin workstation or jump server you have listed as a safe place for Tier 0 accounts to sign in from.

Honey account (decoy)
An account that nothing legitimate uses, so any use of it is an alert.

Silent change
A change found by comparing scans that has no matching event in the Security log: made while auditing was off, or the log was cleared.

gMSA

Group managed service account: a service account whose password Windows creates and rotates, usable only by the servers you name.

Live Watch

Hisn's reading of the DC Security logs every minute or so, between scans.

Not evaluated

A check whose data could not be read. It is never counted as passed.

Fix and rollback scripts

PowerShell generated by Hisn for an administrator to review and run; Hisn never runs them.