Guardian One User Guide

Guardian One documentation | Version 1.1 | Reviewed 30 July 2026

Purpose and Audience

Current version	1.1
Last reviewed	30 July 2026
Document owner	Product owner: Adam Timothy
Change summary	Manager-readability and controlled-publication review

Version history

Version	Date	Change	Status
1.0	Initial issue	Initial controlled document	Superseded
1.1	30 July 2026	Manager-readability and publication review	Current

This guide explains how an authorised customer user opens Guardian One, reads an individual SQL Server assessment, reviews the enterprise estate, filters compliance evidence, and prepares a contact or registration request. Reports contain evidence collected during scheduled point-in-time assessments.

Version History

Version	Date	Change
1.2	13 August 2026	Added subscription warning, grace, suspension, retained-data access and offline renewal instructions.
1.3	14 August 2026	Added Portal port configuration and governed bulk machine-template import.
1.1	30 July 2026	Replaced source-only commands with the verified installed configuration, assessment and licence-request workflow.
1.0	30 July 2026	Initial controlled user guide.

How Assessments and Reports Are Created

Guardian One reports are created from a scheduled assessment, not by the web portal scanning SQL Servers when a user opens a page. The normal workflow is:

- An administrator configures the central Guardian One Windows machine with the central repository, approved authentication, timeouts, and either one SQL Server target or an approved estate target catalogue.
- Guardian One verifies the signed licence and required service entitlement before any collector runs.
- The administrator or Windows Task Scheduler runs C:\Program Files\Guardian One\Assessment\GuardianOne.exe. With no SQL_SERVER environment override, it assesses every enabled configured target; a non-zero exit code means that at least one target failed or the run could not start.
- The command displays timestamped stages while Guardian One collects bounded, read-only SQL evidence and automatically attempts Windows evidence from the target machine. A blocked Windows or WinRM path is recorded as unavailable and does not stop SQL collection.
- Guardian One stores the assessment run, inventory, evidence, findings, recommendations, health result, confidence, and collection limitations in the central SQL Server repository.
- The enterprise portal queries that stored data and constructs the requested HTML page. HTML is not stored in the database. An optional standalone HTML file may also be created when the customer needs a portable report for controlled sharing.

The installed assessment CLI reads the protected estate-targets.json created by Guardian One Configuration and starts each enabled SQL Server assessment in an isolated child process. A failure on one target is reported in the final summary and does not prevent later targets from running. The catalogue contains server names, optional diagnostic-tool settings, and optional non-secret backup-governance policy; do not place usernames, passwords, connection strings, or other secrets in it. All child assessments write to the configured repository. Source-checkout MAIN*.cmd files are development conveniences and are not the installed scheduling contract.

The central service identity requires repository access and read-only assessment permissions on each target SQL Server. When a target resolves to the Guardian One collector machine, the fixed Windows evidence block runs locally under that identity and does not require WinRM. Remote Windows evidence additionally requires the approved WinRM/CIM configuration, firewall access, name resolution, and Windows permissions. A Windows access failure is recorded cleanly as unavailable evidence; SQL-derived assessment continues and missing Windows data is never treated as a pass.

What “Collecting central Windows machine evidence” means

This stage establishes a bounded, point-in-time view of the Windows machine hosting the SQL Server. Guardian One first associates the SQL instance with its current Windows host, then attempts to read operating-system identity and start time, processor topology and current CPU utilisation, physical and virtual-memory availability, page-file usage, fixed volumes and mount points, free capacity, file-system type, and a short disk-throughput and latency snapshot. These facts support the Machine Summary, storage headroom, capacity context and machine-template comparison; they are not continuous monitoring.

The collection runs from the central Guardian One machine under the approved runtime identity. It uses the local Windows path when the SQL Server is on that machine and the customer-approved remote-management path for another Windows host. It does not install an agent, change Windows or SQL Server settings, restart services, read application files, or collect file contents. The implementation commands are intentionally not published in customer documentation; the supported evidence contract and permissions are the stable interface.

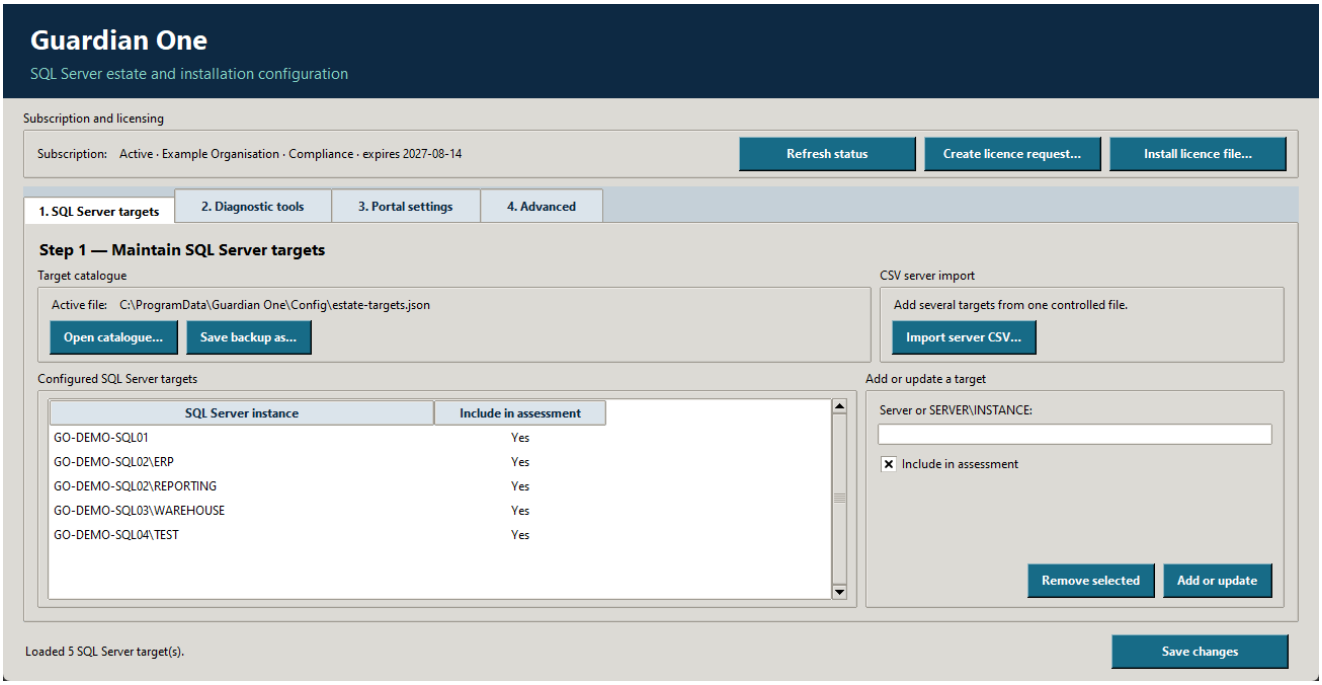
Each evidence group succeeds or fails independently. Guardian One records complete, partial, unreachable, authentication-failed, permission-denied or unsupported status as appropriate. A Windows failure reduces the evidence available for machine conclusions, but the SQL assessment continues and the missing scope is never

reported as healthy or compliant.

Portable Assessment Mode

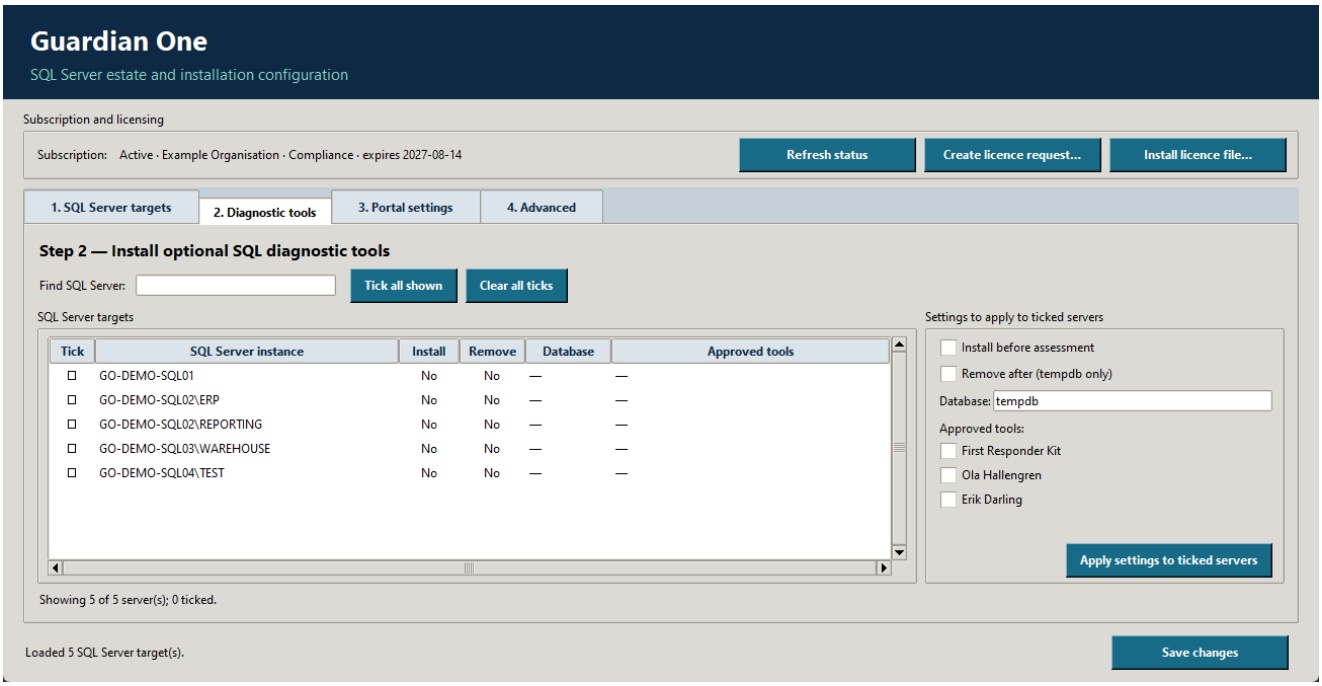
Portable Assessment Mode performs the same live, read-only assessment against real SQL Server targets without requiring a separate SQL Server repository. It stores the authoritative assessment JSON and its SHA-256 integrity digest in a local SQLite database. HTML remains an optional generated export and is not stored in SQLite.

For an installed build, open Guardian One from the Windows Start menu, add the approved target, then save the configuration. Use the dedicated Diagnostic tools step only when the customer approves optional procedure installation. Signed pack installation and rollback are separated into Advanced so routine target and tool settings remain uncluttered. Install an approved offline .gopack there before enabling deployment; Guardian One verifies it and retains the former pack for rollback. Monthly toolkit updates do not replace the Guardian One EXEs. To run the assessment from a console, use:



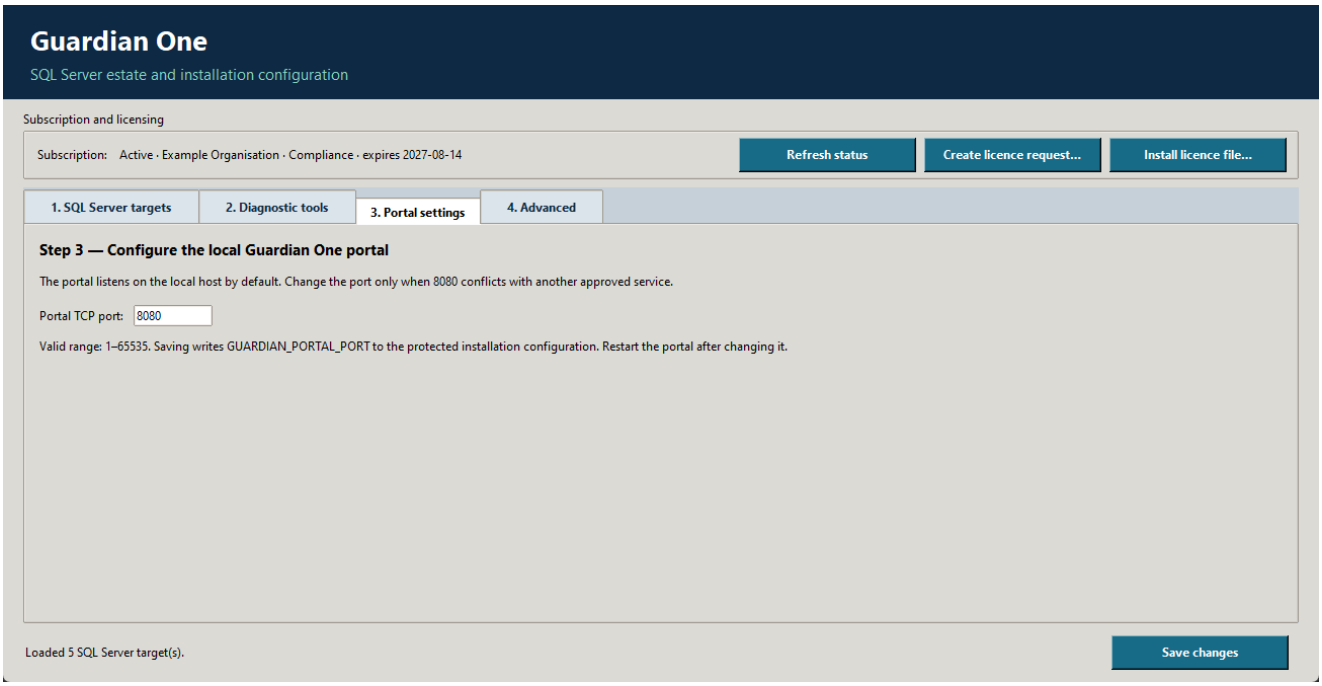
Configuration Step 1 showing the fictional SQL Server target catalogue

The CSV import action appears once on Step 1. SQL Server names are left-aligned for scanning, and Remove selected sits immediately before the primary Add or update action. CSV format rules and duplicate handling are documented below rather than repeated on the form.



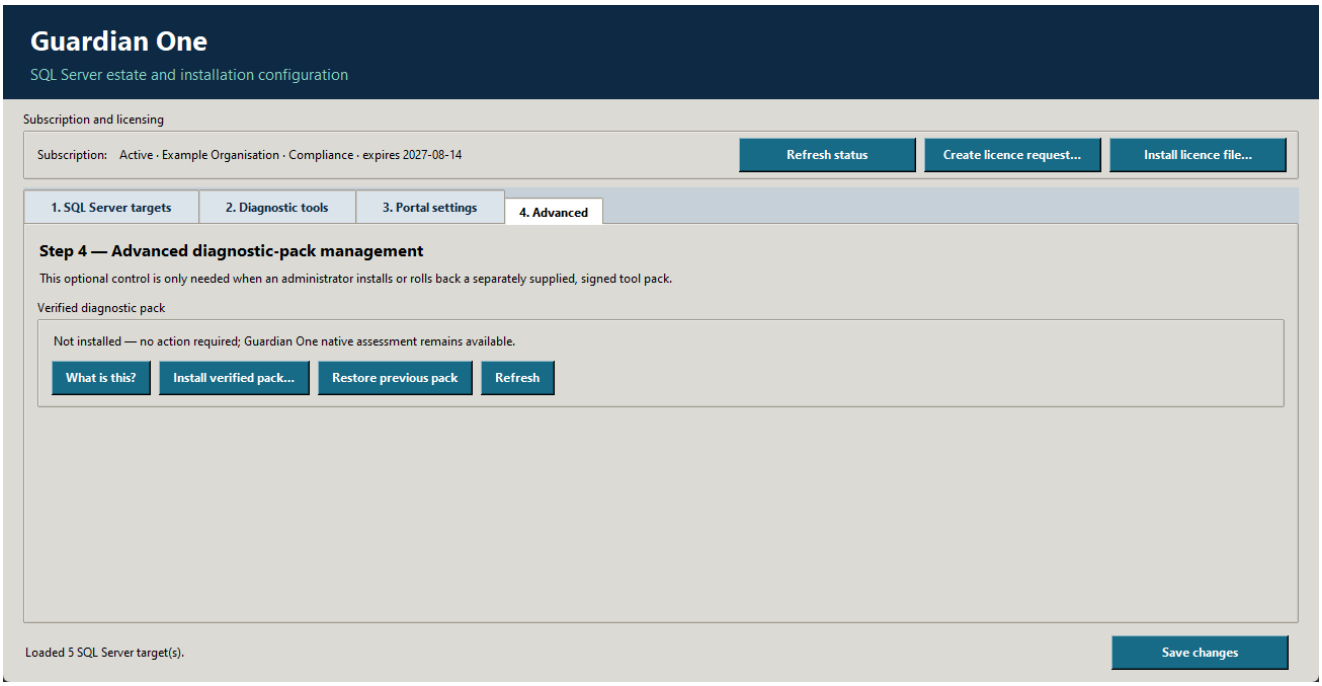
Configuration Step 2 showing the server table and aligned diagnostic-tool settings

Step 2 is optional. Tick one or more SQL Server rows, choose the approved settings, and apply them to the ticked rows.



Configuration Step 3 showing the local portal port

Step 3 keeps the default local port at 8080 and permits an administrator to select another free, approved port. Save changes and restart the Portal application after changing it.



Configuration Step 4 showing the separately grouped advanced diagnostic-pack controls

Step 4 is only for installing or rolling back a separately supplied signed Diagnostic Tool Pack. “Not installed — no action required” means the native Guardian One assessment remains available.

Set-Location 'C:\Program Files\Guardian One' .\GuardianOneAssessment.cmd --portable --open-report

Open one report without the portal

The portal is not required to read an individual report. Every completed installed assessment writes a self-contained HTML file to C:\ProgramData\Guardian One\Reports. Press Windows+R, enter %ProgramData%\Guardian One\Reports, and open the file whose machine and SQL Server instance names match the required target. The filename ends with the assessment date and time. The report opens directly in the default browser and can be copied to a customer-approved location for controlled sharing.

To create and immediately open a new report from the command line, use --open-report. To assess only one SQL Server through the graphical workflow, enable only that target in Configuration before starting the assessment.

Scheduled command-line assessments

The installer provides both the assessment executable and a short CLI launcher. To run every enabled server configured in Guardian One Configuration:

& 'C:\Program Files\Guardian One\GuardianOneAssessment.cmd'

For Windows Task Scheduler, use the executable directly:

- Program/script: C:\Program Files\Guardian One\Assessment\GuardianOne.exe
- Start in: C:\Program Files\Guardian One\Assessment
- Arguments: leave empty for a normal retained assessment, or use --portable only for an approved Portable deployment.

Run under the approved Guardian One service identity, select Run whether user is logged on or not, and choose a customer-approved repeat interval. Exit code 0 means every configured target completed, 1 means one or more targets failed or an unexpected error stopped the run, 2 means configuration or entitlement prevented startup, and 130 means an operator stop was honoured. Reports and repository evidence are retained in the configured locations; the command does not require an interactive desktop.

The installed configuration is held under C:\ProgramData\Guardian One\Config; customers do not need Python or a source checkout. The Python command is applicable only to an explicitly authorised source deployment.

The default database is C:\ProgramData\Guardian One\Repository\GuardianOne_Portable.db. Set GUARDIAN_PORTABLE_DATABASE to an approved absolute path to change it. Restrict the containing directory to the Guardian One service identity and authorised administrators, and use customer-approved disk encryption where required; standard SQLite is not itself an encrypted database.

An unlicensed installation can register at most five distinct SQL Server instance identities over its lifetime, whether it uses Portable SQLite or Full SQL Server repository mode. Signed production licences take their target capacity from the highest enabled service level: Foundation allows 100 targets, Advisor 250, Compliance 500, and Quantum 1,000. In every case the limit counts distinct SQL Server names, not the number of assessment reports run - reassessment of an already-registered identity is unlimited and never consumes another slot. Guardian One provides no delete, slot-reset, replacement or import function. A genuinely new identity over the limit is rejected before an assessment record is created.

Administrator and Reader Responsibilities

- Administrators configure targets, credentials or service identities, schedules, repository access, Windows access, retention, licensing, and customer-managed portal publication controls.
- DBAs and technical owners review collection status, evidence, risks, recommendations, and proposed changes.
- Report readers use the portal and exported reports; opening or filtering a report does not start a new assessment.

Before You Start

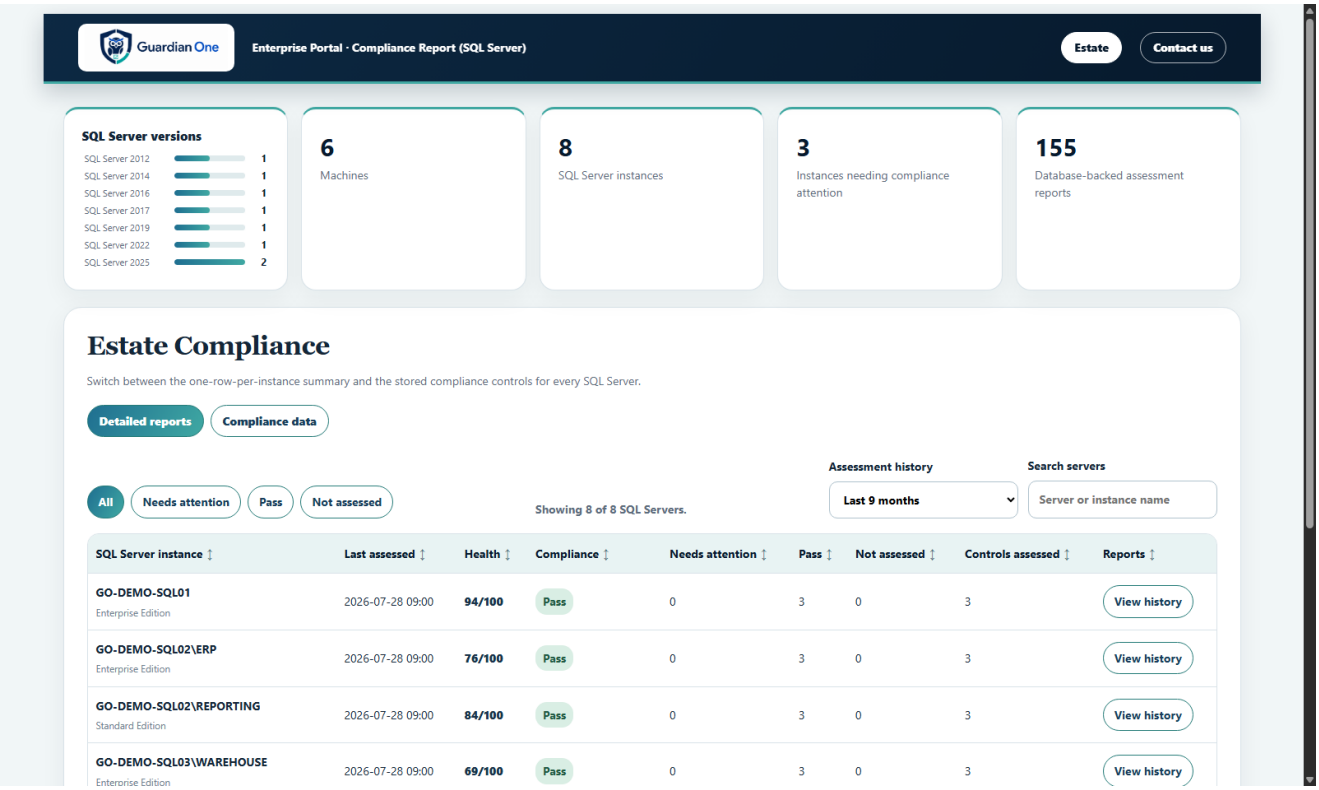
- Confirm that the central Guardian One Windows machine can reach the SQL Server repository.
- Guardian One encrypts SQL Server connections and validates the server certificate by default. Install the issuing root and intermediate certificates in the Windows trust store and ensure the certificate name matches the configured SQL Server endpoint. SQL_TRUST_CERTIFICATE=true bypasses certificate-chain and name validation and is therefore an explicitly approved compatibility exception, not the commercial default. Record the exception, restrict its duration, and restore validation after correcting the SQL Server certificate configuration.
- For estate collection, copy config/estate-targets.example.json to the ignored config/estate-targets.json, approve the server list, and set SQL_REPOSITORY_SERVER to the central repository SQL Server. Keep authentication under the Guardian One process identity or an approved secret store, never in the catalogue.

For Compliance data-movement review, add a backup_governance object to each target. Set environment to one of production, preproduction, staging, uat, test, development, disaster_recovery, or demonstration; list approved backup path/URL prefixes in approved_backup_destination_prefixes; and, for lower environments, list approved production restore sources in approved_restore_source_servers. Guardian One compares aggregate 180-day msdb history with these explicit boundaries. It reports counts, not backup filenames or server names, and treats missing policy as review required rather than inventing an environment from naming conventions.

- Confirm that a valid installation-bound licence enables the required service level.
- Use the customer-approved Guardian One website address. The local portal defaults to port 8080. Setup and Guardian One Configuration → Portal settings can select another free port from 1 to 65535; restart the portal after changing it. Internet or intranet publication, TLS, authentication, firewall rules, and availability are managed by the customer.
- Treat “Not assessed” as unavailable evidence, not as a pass. Review the collection-status explanation and correct permissions, firewall, WinRM, or configuration where appropriate.

Open the Enterprise Portal

Select Sample Enterprise Portal on the original website or open /estate.html at the same address, for example http://server-name:8080/estate.html. The opening page is the Detailed reports view. The header provides clear Estate and Contact us navigation. Summary cards show SQL Server versions, machines, SQL Server instances, assessments, and servers needing attention.



Enterprise Portal opening page

Select a SQL Server version segment to filter the estate to that release. Select it again to clear the version filter. Use the search box to find a machine, SQL Server instance, or relevant report entry.

Choose the Assessment Period

Use Assessment history to select the evidence period:

- Most recent shows only the latest assessment for each SQL Server.
- Today shows assessments recorded since the start of the current day.
- Last 24 hours uses a rolling 24-hour window.
- The 3, 6, 9, and 12 month options support trend and governance review.
- All includes every retained assessment available to the portal.

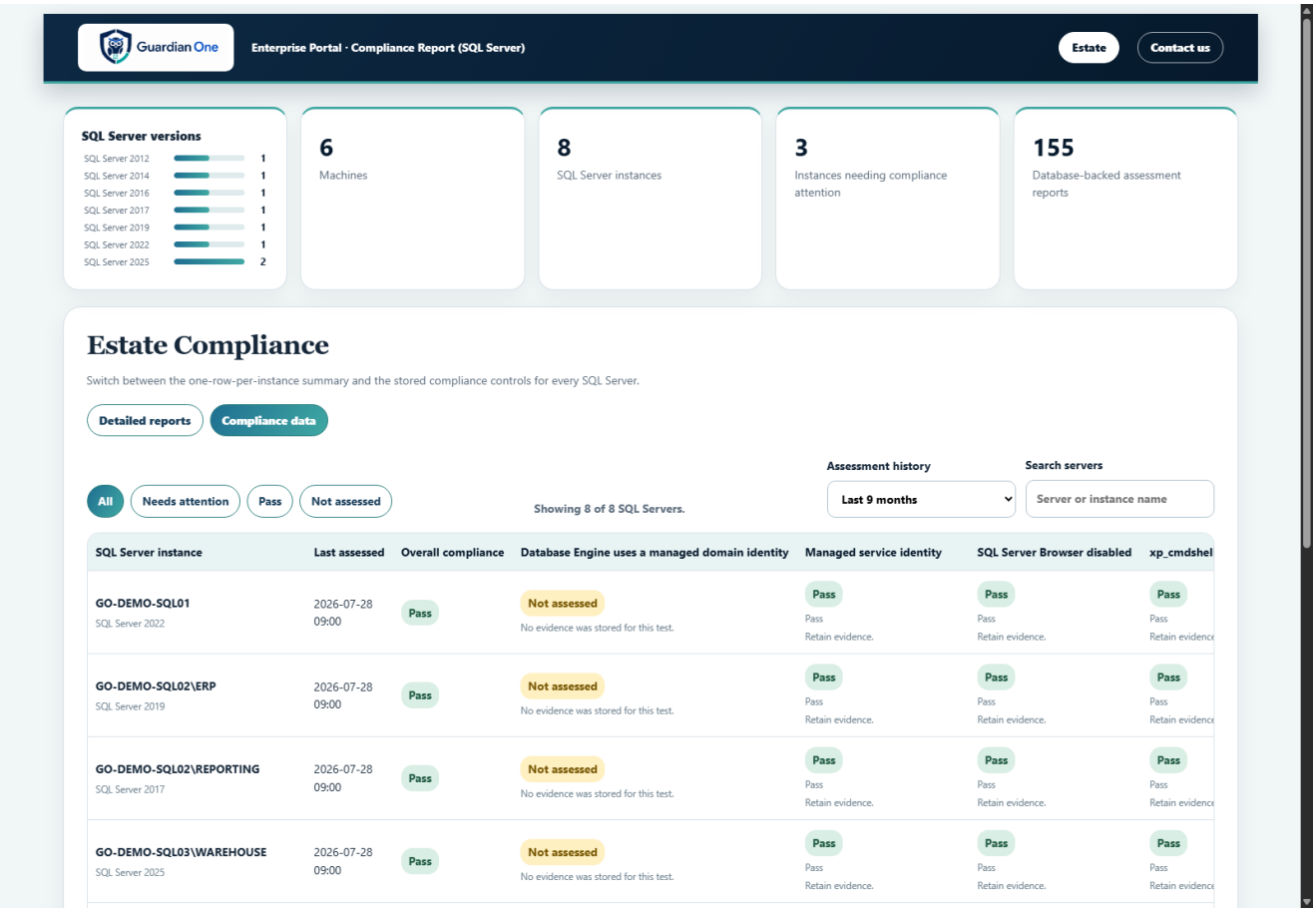
The demonstration estate retains seven approved monthly assessments per SQL Server from January through July 2026. Customer repositories retain history according to the approved customer policy.

Review Detailed Reports

Detailed reports is the default estate view. Each row represents an assessment report and links to the full database-backed HTML report. Select a column heading to sort; select it again to reverse the order. Open report reconstructs the report from stored assessment data and does not require an HTML file in a reports folder.

Review Compliance Data

Select Compliance data to see one row per SQL Server. Each distinct compliance test appears as a column, making differences across the estate visible without opening every full report.



One-row-per-server compliance matrix

Use All, Needs attention, Pass, and Not assessed to filter SQL Servers by the statuses present in their test columns. Matching cells are highlighted. The result message confirms how many SQL Servers are visible. “Not assessed” identifies missing or unavailable evidence and must not be interpreted as healthy or unhealthy.

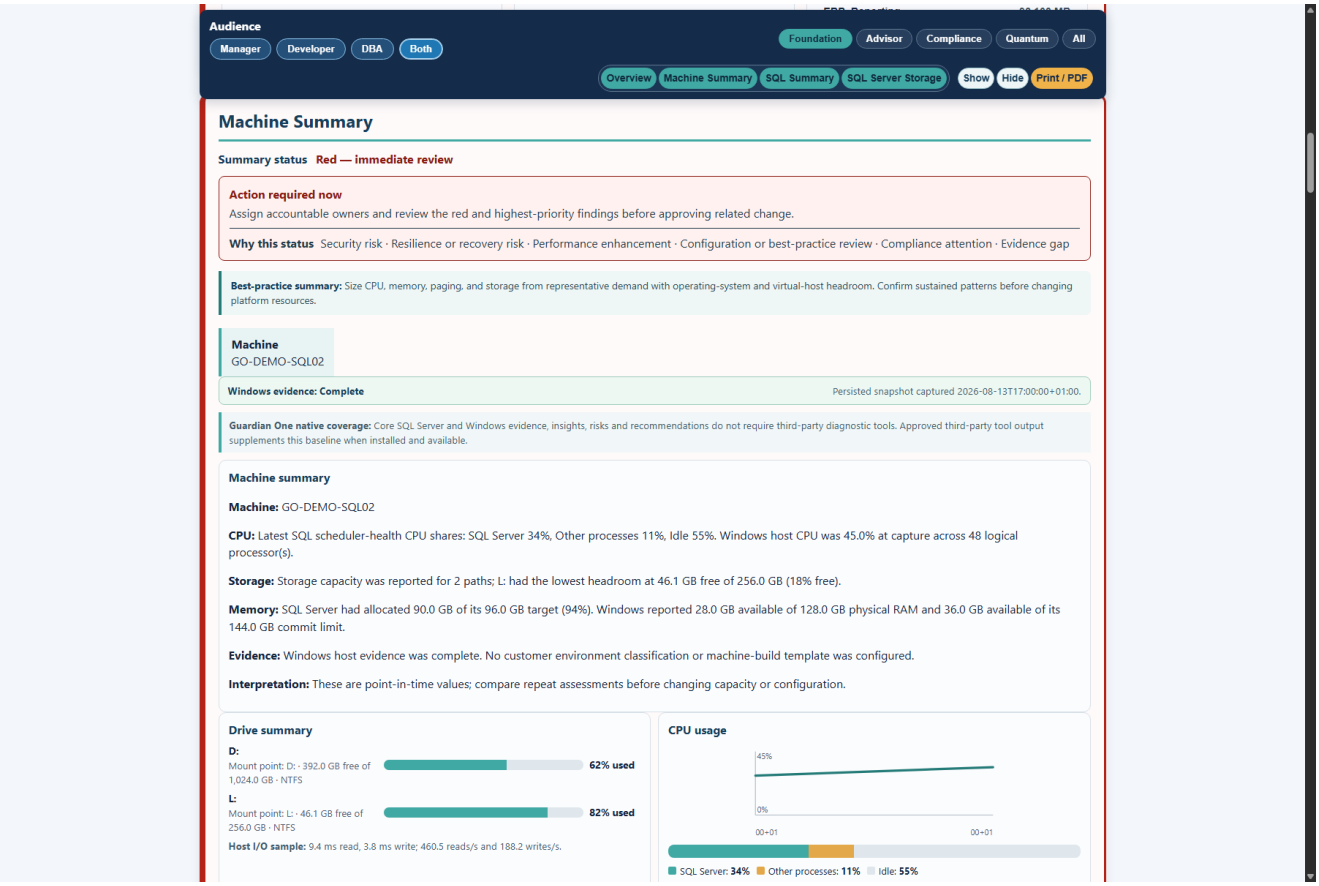
Compare Changes Since the Previous Review

This function is available only with Guardian One Compliance or Guardian One Quantum. Select Changes since review in the enterprise-portal header or open /compliance-changes.html. Choose the previous and current review dates, then select Compare reviews. Guardian One uses the latest completed assessment at or before each date for every SQL Server, accommodating estates whose instances are assessed on adjacent days.

The page separates new failures, resolved failures, persistent failures, exception changes, and unavailable or restored evidence. Changes only is the default; All controls includes unchanged passes and continuing conditions. Foundation and Advisor licences are denied by the server before comparison evidence is loaded, even if a user enters the page address directly.

Read an Individual Assessment

The full report opens with Guardian One branding and defaults to All services. Use Foundation, Advisor, Compliance, Quantum or All to change the content shown. Foundation contains the core inventory and health evidence; Quantum is the governed-AI presentation area. Use Manager for the RAG status, action reasons, senior-management and compliance interpretation, Overview and Business Risk without technical detail. Developer, DBA and Both expose the corresponding technical sections, which remain available when the reader changes audience.



Individual SQL Server assessment report

Review the summary before the detail sections. Findings should include the observed evidence, risk, recommendation, confidence, and any collection limitation. Machine insights distinguish SQL-derived evidence from automatically attempted Windows evidence. When Windows access is unavailable, the report retains SQL-derived value and states clearly that Windows metrics were not assessed.

Use the section buttons to review SQL Server, machine and storage, application databases, maintenance, performance, security, compliance, third-party diagnostic evidence, and recommendations. Third-party procedures such as Brent Ozar or Erik Darling tools can enrich the assessment, but their absence must not remove Guardian One's native findings and recommendations.

Within SQL Server Summary, review SQL Server and SQL Agent Log Issues. Guardian One reads a bounded time window from the configured errorlog.* and SQL Agent log archives through the remote SQL Server connection. The table groups classified issues, counts, latest observation, risk, and recommendations. It does not retain raw messages, principal names, addresses, paths, job details, query text, or other unrestricted log content. A partial, unavailable, or permission-denied status is not a pass; correct access or retention and reassess.

Within Activity Overview, Native operational assessment adds bounded SQL Agent job-failure history, plan-cache review candidates identified by query hash, scheduler pressure, SQL Server process-memory state, and system-health deadlock timestamps. Query text, execution plans, login names, host names and application

identities are excluded. Plan-cache and scheduler evidence is volatile or cumulative since reset and must not be interpreted as a durable trend.

The default log scope requests seven days, attempts up to ten current/archive files independently for SQL Server and SQL Agent, and reviews up to 5,000 rows per source. The report states the earliest and latest evidence actually observed. If log recycling or retention provides less than seven days, Guardian One records insufficient history rather than implying the requested week was assessed.

The assessment identity must be permitted to read SQL Server and SQL Agent error logs. On SQL Server 2022 and later, use the supported least-privilege server permission where available; older versions may require membership of a privileged fixed server role or a customer-approved, certificate-signed wrapper. Do not grant sysadmin solely for Guardian One log collection. Test the permission on every supported SQL Server version, restrict it to registered targets, and record denied access as unavailable evidence rather than broadening privileges automatically.

Storage and Mount Points

Machine Summary includes the Windows domain, operating-system identity and host start time when the corresponding Windows evidence is available. Machine storage includes drive letters and volume mount points. Review total space, free space, utilisation, and workload purpose. A collection failure is shown as unavailable evidence with corrective guidance; it does not stop SQL-derived assessment and does not create a false pass.

Customer Machine Templates and Report Content

Authorised repository administrators can define machine-build templates by environment class and domain. A template lists required or optional drive letters and mount points with their intended purpose. Machine-name rules then assign a collected host to the highest-priority matching template. For example, a contains DEV rule can classify UKSQLDEV01 as Development, while contains DEMO can classify UKSQLDEMO02 as Demonstration.

The Machine Summary records the resolved environment, matching template, matched volumes, missing required volumes, unexpected volumes, risk, and recommendation. If no naming rule matches, or Windows evidence is unavailable, the comparison is explicitly not configured or not assessed; it is never presented as a pass.

The enterprise portal’s Detailed reports table shows the environment and machine-template outcome stored with each latest assessment. Historic assessments that predate this evidence remain Not assessed; the portal does not retrospectively apply current templates and imply that an earlier machine conformed.

The customer may also enable or disable individual report blocks through dbo.usp_SetReportPresentationSetting. Available settings cover CPU, drives, mount points, machine memory, SQL Server memory, the natural-language machine summary, SQL Server storage locations, and each detailed Activity subsection. Hiding a block does not stop its collector and does not delete its repository evidence.

Use the controlled procedures installed by migration 018 to create or update templates, expected volumes, naming rules, and report settings. Apply more-specific naming rules at a lower priority number. Review rule overlap before production use so names such as pre-production and production cannot be classified by an unintended broad substring.

Portal users can view this configuration at /machine-templates.html or select Machine templates from the enterprise-portal header. The page also previews the environment and template selected for a proposed machine name.

For a small number of templates, use that page to add each template, its expected volumes and its name-classification rules. For a large estate, prepare a reviewed JSON file and use the installed Configuration command line. Preview is the default and makes no repository change:

& 'C:\Program Files\Guardian One\Configuration\GuardianOneConfiguration.exe' --import-machine-templates 'D:\ApprovedTransfer\machine-templates.json'

After the preview counts match the approved change, apply the same file transactionally:

& 'C:\Program Files\Guardian One\Configuration\GuardianOneConfiguration.exe' --import-machine-templates 'D:\ApprovedTransfer\machine-templates.json' --apply-machine-templates

The command requires the normal configuration_changes entitlement, validates the entire file before connecting, uses only the governed repository procedures, parameterises every value, and commits all templates together or rolls back the complete import. It does not require internet access and must not be replaced by direct table edits.

Example input with fictional names:

{ "templates": [{ "template_name": "Production SQL", "environment_class": "Production", "domain_name": "example.test", "description": "Approved production SQL host layout", "volumes": [{ "volume_kind": "drive", "volume_path": "D:\\", "purpose": "Data", "is_required": true, "display_order": 10 }], "rules": [{ "match_type": "contains", "pattern": "PROD", "priority": 10 }] }] }

Valid volume_kind values are drive and mount_point. Valid match_type values are contains, prefix, suffix and exact. Lower rule-priority numbers are evaluated first. Review broad patterns and overlaps before applying them, then run one assessment per environment class and confirm the resolved template and volume comparison in the report.

Administrative changes remain locked unless GUARDIAN_ONE_PORTAL_ADMIN_TOKEN is set in the portal host environment or its protected config/.env, followed by a portal restart. Use a unique high-entropy value, restrict

the page to authorised administrators, and require HTTPS through the customer-managed reverse proxy before entering the token. The token is checked server-side and is not stored in the repository or returned in the page.

Governed Compliance Exceptions

A failed compliance control may have a formally approved exception, but it must never be changed to Pass. Open Compliance exceptions from the enterprise-portal header or browse to /compliance-exceptions.html. The current register appears before the administration form and identifies active, inactive and expired entries. Repository administrators can use that form or dbo.usp_UpsertComplianceException to record the exact control name, optional SQL Server scope, two different agreeing parties, reason, approval date, review date, active state, and the person making the repository change. An omitted server scope applies estate-wide and therefore requires especially careful approval.

During assessment Guardian One applies only active exceptions whose approval and review dates include the assessment date. The stored and rendered result becomes Approved exception, while retaining Needs attention as the underlying result. Reports show the agreeing parties, reason and review date. When the exception is disabled or its review date expires, a continuing failure returns automatically to Needs attention.

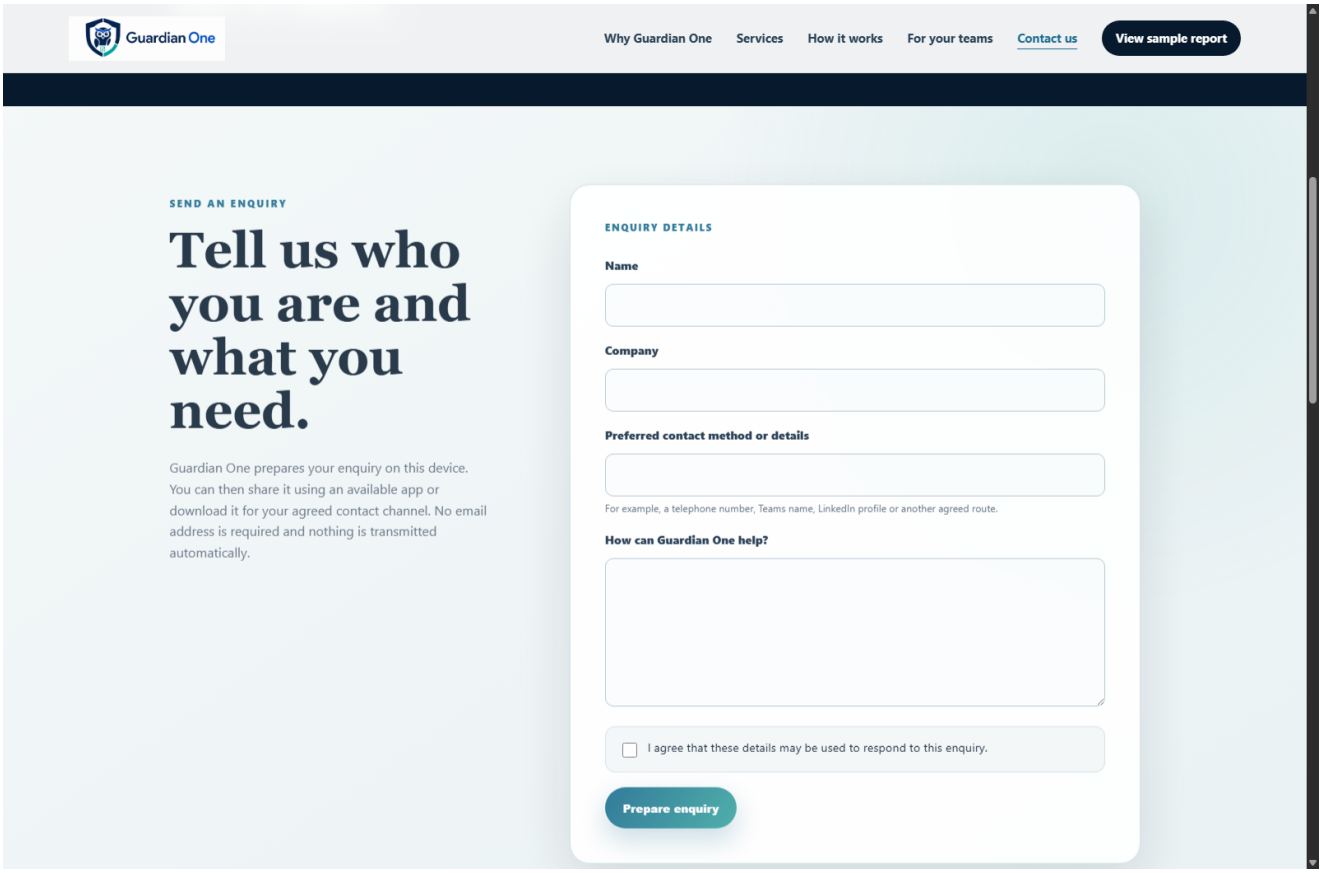
Example:

EXEC dbo.usp_UpsertComplianceException @ServerName = N'UKSQLPROD01', @ControlName = N'Local service account', @AgreedByA = N'Application service owner', @AgreedByB = N'Information security owner', @ExceptionReason = N'Approved isolated legacy service pending migration', @ApprovedDate = '20260729', @ReviewDate = '20261201', @IsActive = 1, @ChangedBy = N'Guardian One administrator';

Do not put passwords, personal notes or unrelated sensitive material in exception fields. Review expired and approaching-review exceptions as part of the customer’s governance process.

Contact and Registration Requests

Select Contact us. Enter name, company, preferred contact method, and the request details. Guardian One prepares the enquiry locally. The browser may offer the operating-system share function; otherwise download the prepared text and forward it using the agreed contact route. The page does not send personal data automatically and does not use a fixed sales email address.



Contact request form

For an installed build, open Guardian One from the Start menu. In the grouped Subscription and licensing section, select Create licence request. The application collects the contact name, company and preferred contact route, then creates a JSON request and a readable text copy in the user's Documents\Guardian One Licence Requests folder. It does not send either file automatically.

An administrator may alternatively run this packaged command:

& 'C:\Program Files\Guardian One\Assessment\GuardianOne.exe' --registration-request --name "Alex Smith" --company "Example Ltd" --contact "Telephone or agreed contact route"

Subscription Status and Offline Renewal

Guardian One Configuration shows the current signed subscription state:

- Active — normal licensed work is available.
- Warning — normal work continues, but install the renewed signed licence before the displayed expiry.
- Grace — normal work continues temporarily after expiry until the displayed grace end.
- Suspended — new assessments, target/configuration changes, evidence collection, new report generation and AI processing stop. Existing reports and repository evidence are not deleted. A Compliance or Quantum enterprise portal remains available for retained report reading, with its administration controls disabled.

To reactivate an installation, obtain the renewed machine-bound .key file through the approved fulfilment route. Open Guardian One Configuration and use Install licence file beside Create licence request in the Subscription and licensing section. Choose the file and confirm the displayed state and expiry. Guardian One validates it before changing the installed licence and retains the previous file as licence.key.previous. Restart any already-running assessment or portal process so it loads the renewed entitlement. This flow does not require internet access from the SQL Server or Guardian One host.

Warning and grace lengths are signed into the licence. Do not attempt to change dates, replace the protected state, move the system clock backwards or reinstall an older licence. Those conditions suspend new work and require Operations review. They do not remove retained customer data.

Licence Failure Messages

Guardian One denies new assessment work when the licence is malformed, tampered with, not yet valid, for another machine, outside its product-version range, replayed after a newer licence, or missing the required entitlement. A licence beyond grace enters suspended retained-data mode; it does not silently start a new demo. A denied start does not run collectors or create assessment data. Follow the displayed registration or renewal guidance and provide the generated installation identifier through the agreed contact route.

Copying the application and its licence to a Windows machine with a different MachineGuid does not transfer the entitlement. Planned licence transfer, disaster recovery, and revocation procedures must be agreed before production release.

Interpreting Results Safely

- Treat recommendations as decision support; validate changes in a non-production environment and follow customer change control.
- Prioritise immediate risks, then high-attention findings, while considering business criticality and dependencies.
- Do not infer a pass from missing Windows, SQL, third-party, or application evidence.
- Retain assessment history according to the customer’s approved governance and data-retention policy.
- In Portable Assessment Mode, back up the SQLite file as one protected unit; do not copy it while a write is active or edit it with general SQLite tools.
- Escalate unexpected gaps or conflicting evidence to the responsible DBA or platform owner.

Troubleshooting

Common Operational Questions

- Is a website required? No. Assessments, persistence and standalone HTML generation operate without a web front end. The enterprise portal is an optional database-backed presentation and administration layer.
- Can Portable Demo Mode use the enterprise portal? Yes. The local portal reads integrity-checked retained evidence from the Portable SQLite repository. Standalone HTML reports remain available and do not require the portal.
- Can SQL Server authentication credentials be put in .env? No. The current release supports Windows integrated authentication. SQL usernames and passwords must not be stored in Guardian One configuration or evidence. A customer requiring SQL authentication needs an approved vault-backed implementation before deployment.
- Are the assessments real? Yes. Portable mode queries the approved target SQL Server; only the result-storage technology changes.
- Can a portable slot be freed? No. Five canonical identities can be reassessed indefinitely, but slots cannot be deleted, replaced, imported or reset through the supported product.
- Does unavailable Windows evidence stop the report? No. SQL-derived assessment continues and the missing Windows scope is clearly marked as not assessed.
- Are third-party tools mandatory? No. Guardian One retains native evidence and recommendations without them.
- Portal unavailable: confirm the service is running, the configured bind address and port are correct, and the customer-managed firewall or reverse proxy permits access.
- No reports visible: confirm the portal points to the intended repository and that assessments have committed successfully.
- Report link opens the wrong location: use the portal’s database-backed Open report link rather than a file-system directory listing.
- Windows evidence unavailable: Guardian One attempts safe collection automatically. For the collector machine, verify that the runtime identity can read local CIM and performance counters. For a remote host, also verify WinRM, firewall rules, DNS and the approved remote permissions. Review the assessment log for the classified failure; SQL-derived evidence remains available.
- Licence denied: generate a registration request and check the licence ID, machine binding, validity dates, product version, and enabled service levels.