

SQL Change Guard Installation and Operations Guide

This guide is for the IT, DBA and security teams who install and operate SQL Change Guard. It describes the installation step by step and explains every setting of the corporate directory (LDAP), corporate sign-in (SSO), ITSM and SIEM integrations: which values each setting accepts and where the information that comes from the other system is written in the product. What must be prepared before installation is in the Installation Prerequisites Checklist. How to use the screens is in the User Guide.

1. Parts of the product	5
2. Where settings are kept	6
2.1 Secrets are kept in environment variables.....	6
2.2 Secret list.....	7
2.3 Generating keys.....	8
3. Database installation.....	10
3.1 Way A: the product installs (AutoMigrate = true, the default)	10
3.2 Way B: the DBA installs (AutoMigrate = false)	10
3.3 Three tasks for the DBA after installation	10
3.4 Ledger digest store.....	11
3.5 Evidence ledger	11
4. API installation	14
4.1 Core settings.....	14
4.2 Email.....	16
4.3 Timestamp (optional).....	17
4.4 Approval chain and governance state.....	18
5. Worker installation.....	19
6. Web interface, licence and first sign-in.....	21
6.1 Web interface.....	21
6.2 Licence	21
6.3 First sign-in	21
7. Corporate directory (LDAP / Active Directory).....	22
7.1 How it works	22
7.2 Settings (appsettings.json, Ldap section).....	22
7.3 What is read from the directory and where it is written	24
7.4 Group to role mapping.....	24
7.5 Synchronisation.....	25
7.6 Lockout threshold	26
7.7 Installation order	26

8. Corporate sign-in (SSO)	27
8.1 How it works	27
8.2 General settings (appsettings.json, Sso section)	27
8.3 Identity provider settings (Sso:Providers list)	28
8.4 What is read from the assertion and where it is written	29
8.5 Group to role mapping.....	30
8.6 What to do at the identity provider	30
8.7 Installation order	31
9. ITSM integration.....	32
9.1 How it works	32
9.2 Connection settings (appsettings.json, Itsm section)	32
9.3 ServiceNow: what is read and where it is written	33
9.4 Jira and other ITSMs: what is read and where it is written	34
9.5 How the state is interpreted (StateClass)	36
9.6 Behaviour parameters (Settings > Parameters > ITSM Ticket)	38
9.7 The note written to ITSM	40
9.8 Installation order	40
10. SIEM / SOC integration.....	42
10.1 How it works	42
10.2 Connection settings (appsettings.json, Siem section)	42
10.3 Behaviour parameters (Settings > Parameters > SIEM)	43
10.4 Event fields	44
10.5 Installation order	45
11. Installation verification	46
12. Operations.....	48
12.1 Logs	48
12.2 Backup.....	48
12.3 Upgrading.....	48
12.4 Changing keys.....	49

12.5 Trace of settings file changes	49
12.7 Ledger digest and evidence write boundary	50
12.8 Common problems	51

1. Parts of the product

Part	File	How it runs
Web interface	Static files (index.html and the assets folder)	A separate site on IIS. No .NET needed
API	SCG.API.dll	ASP.NET Core application on IIS. Application pool: No Managed Code
Worker	SCG.Workers.exe	Windows service
Application database	SQL Server 2022 or later	All records of the product. Audit records are kept in an append-only ledger table; the database engine rejects UPDATE and DELETE on this table (Section 3.5)

Who connects to whom:

Browser --443--> Web interface (static files)

Browser --443--> API

Worker --443--> API (configuration, ITSM notes, directory sync, execution decisions)

API, Worker --1433--> Application database

API --> Ledger digest store (immutable folder)

API, Worker --> Target databases (SQL Server, PostgreSQL, Oracle)

API --> Corporate directory (LDAP), identity provider (SSO), ITSM

API, Worker --> SIEM collector, SMTP

API --> Timestamp server (if enabled)

Two important rules:

- Only the API connects to the corporate directory, the identity provider and ITSM. The Worker calls the API for this work. The settings and secrets of these integrations are kept only in the API's settings file.
- The Worker's own settings file holds only the API address and the Worker key. It receives the database connection string and the encryption keys from the API at start-up. The evidence signing private key never goes to the Worker: the Worker has the API sign its execution events and only starts the ledger digest round (the API takes, signs and writes the digest). The API signs a Worker notification only after checking it against the approval chain. If the Worker and the API are on different servers, the connection between them must use HTTPS.

2. Where settings are kept

The product's settings are kept in three places. Which setting lives where is a deliberate choice.

Place	What it holds	Who changes it	When it changes
appsettings.json in the API folder	Connections: database, directory, identity provider, ITSM, SIEM, email addresses and timings	The installer	The API is restarted. Changes in the LDAP, SSO and ITSM sections are detected at start-up and written to the audit trail
Environment variables	Secrets: passwords, keys, connection strings	The installer	The API and the Worker are restarted
Settings > Parameters in the product	Behaviour: ITSM and SIEM rules, approval rules, number formats	Application administrator	Takes effect immediately. Written to the audit trail; if settings approval is on, it goes through a second administrator's approval

2.1 Secrets are kept in environment variables

The product reads a setting first from appsettings.json and then from the environment. An environment variable overrides the value in the file. The variable name is the setting path with each colon replaced by a double underscore: the Jwt:SigningKey setting is read from the Jwt__SigningKey variable.

Secrets are not left in the file. In most organisations the file ends up in backups and source control; a secret kept there is in the hands of anyone who can read the file.

Definition (in a command prompt opened as administrator, permanent system variable):

```
setx /M Jwt__SigningKey "value"
```

Removal (setx writes an empty value, it does not remove):

```
reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\Environment" /F /V  
Jwt__SigningKey
```

After a variable is defined, the API and the Worker service are restarted. IIS may not see new system variables when the application pool is recycled; in that case IIS is restarted (iisreset in a command prompt opened as administrator) or the server is restarted. An already open command window does not see the new variable; open a new one. Whether the variable is actually read is checked in the Secret placement group below.

Verification: the Secret placement group on the Settings > Diagnostics > Governance Readiness screen shows, for every secret, where its value comes from: environment variable, configuration file or not defined. The expected value is environment variable. The screen never shows the secret itself.

2.2 Secret list

Required secrets. If one is missing, the product does not start or does not work:

Environment variable	Purpose	How it is produced
ConnectionStrings__Default	Application database connection string	Provided by the DBA
Jwt__SigningKey	Signature of session tokens. At least 32 characters	Random (2.3)
Security__ServerPasswordKey	Encryption of server passwords. Base64, exactly 32 bytes when decoded	Random 32 bytes, base64
Security__QrZipPasswordKey	Encryption of query result package passwords. Base64, exactly 32 bytes	Random 32 bytes, base64
Workers__ApiKey	The Worker identifies itself to the API	Random. The same value is also defined on the Worker side as WorkerApi__Key
WorkerApi__Key	The Worker side counterpart	Same value as Workers__ApiKey

Conditional secrets. Needed only if the related feature is used:

Environment variable	When
Mail__Password	If sending email requires authentication
Ldap__BindPassword	If the corporate directory is used
Sso__Providers__N__ClientSecret	Corporate sign-in with OIDC. N is the provider's position in the list; the first provider is 0
Sso__Providers__N__SpCertificatePassword	If a SAML signing certificate is used
Itsm__Password or Itsm__Token	If the ITSM integration is used
Evidence__Signing__Keys__1__PrivateKeyPem	Signing of evidence files, only if the key is not in the certificate store (2.3). While signing is on (Evidence:Signing:Enabled = true) and no usable key is available, the product starts but evidence dossiers, audit records packages, ledger digests and period packages are NOT produced; no unsigned output is given. The state is shown on the Governance Readiness screen
Evidence__Timestamp__ProxyPassword	If the timestamp server is reached through a proxy that requires a password
ConnectionStrings__Worker	If the Worker connects to the application database with an account separate from the API (section 5). When defined on the Worker server the Worker uses this value; with

Environment variable	When
	Workers:ShareConnectionString = false on the API, the API does not send connection strings to the Worker at all

2.3 Generating keys

A random 32-byte value in base64 (the required format for the Security keys; it can be used for the others too):

```
powershell -NoProfile -Command "$b=New-Object byte[]
32;[System.Security.Cryptography.RandomNumberGenerator]::Create().GetBytes($b);[Convert]::ToBase64String($b)"
```

Evidence signing key pair (RSA 3072):

```
openssl genpkey -algorithm RSA -pkeyopt rsa_keygen_bits:3072 -out priv.pem
openssl rsa -pubout -in priv.pem -out pub.pem
```

The private key (priv.pem) is written to the Evidence__Signing__Keys__1__PrivateKeyPem environment variable. The public key (pub.pem) is not a secret; it is written to Evidence:Signing:Keys:1:PublicKeyPem in appsettings.json and given to auditors. When writing it into JSON, line breaks are written as \n. The fingerprint to give to auditors:

```
openssl pkey -pubin -in pub.pem -outform DER -out pub.der
openssl dgst -sha256 pub.der
```

Recommended for production: the private key is kept in the Windows certificate store, not in an environment variable. Anyone who manages the server can read a key from an environment variable and use it to sign outside the server; a key imported as non-exportable cannot be copied.

1. The key and the certificate are prepared in a .pfx file (from the certificate authority of the organisation or self-signed with openssl, RSA 3072).
2. On the API server the .pfx is imported into Local Computer > Personal with "Mark this key as exportable" switched OFF.
3. Right-click the certificate > All Tasks > Manage Private Keys: read permission is given only to the API application pool identity. The Worker does not sign; it has the API sign its execution events, and the API takes and signs the ledger digest itself.
4. In appsettings.json the thumbprint of the certificate is written to Evidence:Signing:Keys:1:CertificateThumbprint (CertificateStoreLocation: LocalMachine). PrivateKeyPem and Evidence__Signing__Keys__1__PrivateKeyPem are not defined. If PublicKeyPem is left empty it is taken from the certificate.

5. If the organisation has an HSM or TPM, the key is placed in the same store with the vendor's Windows provider; the product setting stays the same.

The "Where the signing key is kept" row on the Governance Readiness screen shows the source of the key. The cost of changing keys is in section 12.4.

3. Database installation

The installation scripts come in the API folder under DbScripts\sqlserver: 001_Tables.sql, 002_SeedData.sql, 003_StoredProcedures.sql, 004_TableWriteLogs.sql. Every applied script is recorded in the SchemaVersions table with its SHA-256 digest. If an applied script is later changed, the product reports an error at start-up and does not start.

There are two ways. The choice is made with the Database:AutoMigrate setting.

3.1 Way A: the product installs (AutoMigrate = true, the default)

1. The application database account is given db_owner on the database. If the database was not created beforehand, the product creates it; the account then also needs dbcreator.
2. On first start the API applies the pending scripts in order. The log shows [Schema] Applying and [Schema] Completed lines for each script. If the database was created, a [Schema] Database created line is written.
3. On later starts only new scripts are applied; the log shows [Schema] The schema is up to date.

3.2 Way B: the DBA installs (AutoMigrate = false)

For organisations with strict change control. In this way the product never touches the schema; it only checks it.

1. The DBA creates an empty database and applies the scripts under DbScripts\sqlserver in number order. When sqlcmd is used, the -I (quoted identifiers on) and -f 65001 (the scripts are UTF-8 and contain Turkish text) options are used:

```
sqlcmd -S SQLSERVER -d DatabaseName -I -f 65001 -b -i 001_Tables.sql
```

2. The DBA runs the DbScripts\DbSchemaVersions.ps1 helper in the API folder:

```
powershell -ExecutionPolicy Bypass -File .\DbSchemaVersions.ps1 -AppliedBy "COMPANY\dba1"
```

The helper does not connect to any database. It produces a SchemaVersions_Register.sql file that contains the digests the product computes for the scripts. The DBA reviews the file and applies it after the scripts.

3. The application account gets db_datareader, db_datawriter and EXECUTE. The account is also added to the evidence ledger role and gets permission to read the ledger views and the definitions in the evidence schema (section 3.5). sysadmin and db_owner are not granted.
4. The API checks at start-up. If a script is missing or changed, it names it and does not start.

3.3 Three tasks for the DBA after installation

Consistent reads. Evidence reports do not use dirty reads; so that they do not wait on locks during heavy writing, snapshot reads are turned on in the application database. This command cannot be put in the

scripts, because the scripts run inside a transaction. It is run once, when there is no other connection to the database:

```
ALTER DATABASE [DatabaseName] SET READ_COMMITTED_SNAPSHOT ON WITH ROLLBACK IMMEDIATE;
```

Ledger verification. When an evidence file is generated, the ledger is verified with `sys.sp_verify_database_ledger`, which requires snapshot isolation. If the product installs the schema (path A) it turns this setting on itself. On the DBA path it is run once:

```
ALTER DATABASE [DatabaseName] SET ALLOW_SNAPSHOT_ISOLATION ON;
```

If the setting is off, the evidence file says "ledger could not be verified"; it never shows "verified".

Protecting the database write log. `004_TableWriteLogs.sql` installs triggers on the tables that also capture changes made by bypassing the application, and writes them to the `TableWriteLogs` table. The application account does not need to change this table. In production:

```
GRANT INSERT ON dbo.TableWriteLogs TO [application_account];
```

```
DENY UPDATE, DELETE ON dbo.TableWriteLogs TO [application_account];
```

3.4 Ledger digest store

Once an hour the Worker starts a digest round; the API takes the digest of the evidence ledger, signs it and writes it to this folder. The folder is the external witness of the evidence: even if someone who manages the database changes records later, the digest written outside does not change, so the change shows up in the auditor's verification.

1. The storage team prepares an immutable folder: a WORM share, storage with object lock, or a share the database administrator cannot write to.
2. The API application pool identity gets permission to create new files and to read; it gets no permission to change or delete files. The database administrator gets no write permission on this folder. When an evidence file is generated the ledger is verified against the file in this folder; if the API cannot read the file the result is `VERIFIED_INTERNAL` (a verification that is not independent).
3. The folder path is written to the `Evidence:Ledger:DigestOutputPath` setting (Section 4.1). The path must be visible from the API server.

The product never overwrites an existing file. If the folder is not defined the ledger still works, but no record is covered by an external digest and the Governance Readiness screen warns. See Section 12.7.

3.5 Evidence ledger

Audit records are kept in the `AuditLogs` table of the evidence schema in the application database. The table is a SQL Server append-only ledger table: the database engine rejects `UPDATE`, `DELETE` and `TRUNCATE` for everyone, `sysadmin` included. This is why the application database must be SQL Server 2022 or later; the ledger exists in every edition (Express included). The ledger table alone does not

protect against returning the database to an older backup; such a return is detected with the digests written outside (Section 3.4).

The installation scripts create:

Object	Purpose
evidence schema	Owned by evidence_owner, a user without a login. An object in the dbo schema (trigger, procedure) cannot write to this table
evidence.AuditLogs	The ledger table. It carries no trigger
evidence.usp_Audit_Append	The only way to write to the table. It sets the event time itself from the database server clock (the caller cannot send a time) and checks the required fields
dbo.AuditLogs	The view that reports and screens read. It is not a write path
evidence_api_writer, evidence_worker_writer roles	Permission to read the table and run the procedure. No INSERT, UPDATE or DELETE on the table

Additional permissions for the application account on the DBA path (3.2). If the API and the Worker use the same account, the account is added to both roles:

```
ALTER ROLE evidence_api_writer ADD MEMBER [application_account];  
ALTER ROLE evidence_worker_writer ADD MEMBER [application_account];  
GRANT VIEW LEDGER CONTENT TO [application_account];  
GRANT VIEW DEFINITION ON SCHEMA::evidence TO [application_account];
```

If the API and the Worker connect with separate accounts, the API account is added only to evidence_api_writer and the Worker account only to evidence_worker_writer. The Worker account then cannot write user decisions such as approval, rejection and sign-in to the audit trail.

Boundary check. At start-up and every 15 minutes the API, and the Worker with its own job, check: is the evidence table a ledger, does it have a trigger, is the write procedure the version the product released, is there an unexpected object in the evidence schema, does another object reference the table, was the table dropped and recreated, is TRUSTWORTHY or DB_CHAINING on. If the evidence table is missing, is not a ledger or the database is older than SQL Server 2022, the API does not start. For the other findings the API starts and screens can be read, but state changing operations such as saving, approving, rejecting and executing requests are not possible until the boundary is restored. The finding is reported with the Evidence.BoundaryBroken event, an email and the log; when it is restored Evidence.BoundaryRestored is written.

Rules for the DBA after installation:

- No object is added to the evidence schema, the write procedure is not changed, no trigger is added to the evidence table. If one of these is done, the product stops change operations.
- TRUSTWORTHY and DB_CHAINING stay off on the database.
- NTP must be on for the database server.
- The DBA should not be an operating system administrator on the database server. Writing schema changes with SQL Server Audit to a channel the DBA cannot reach (Windows security log or SIEM) is recommended.

4. API installation

1. The delivered API folder is copied to the server (for example D:\SQLChangeGuard\api).
2. An application pool is created in IIS: .NET CLR version No Managed Code.
3. A site is created for the API with the API folder as its root. An HTTPS binding and certificate are defined for the API address.
4. The application pool identity is given write permission on the logs folder under the API folder and read permission on the query result file folder.
5. appsettings.json is edited (4.1). Secrets are defined as environment variables (2.2).
6. The application pool is started. Log file: logs\scg-YYYYMMDD.log in the API folder.

4.1 Core settings

The table below lists the settings that are always reviewed during installation. The details of each field are in section 2.4 of the User Guide. The integration settings are in sections 7 to 11 of this guide.

Setting	Value to write at installation	Notes
AllowedOrigins	["https://changepguard.company.local"]	Address of the web interface. Requests from addresses not listed are rejected
Database:AutoMigrate	true or false	Section 3
Display:TimeZone	Europe/Istanbul	Time zone used for times in documents and emails. Records are always stored in UTC
Auth:Password:ResetBaseUrl	https://changepguard.company.local	Root of the link in the password reset email
Auth:Password:MinLength, RequireUppercase, HistoryCount	12, true, 5 (suggested)	Password rules of local accounts
Auth:AccountLockoutMaxAttempts	Lower than the directory's lockout threshold	Section 7.6
Auth:MaxSessionHours	12	Longest duration of a session from the first sign-in. The access token (Jwt:AccessTokenMinutes) and the refresh token (Jwt:RefreshTokenHours) never go beyond it; a refused renewal is written

Setting	Value to write at installation	Notes
		to the audit trail as a SessionRefreshRejected event
Mfa:Enabled, Mfa:EnforceEnrollment	true, per organisation	The product's two-step verification for local and directory accounts
Mail:Enabled, Mail:DevMode	true, false	If DevMode stays on, all emails go to a single test address
QueryResult:OutputPath	D:\SQLChangeGuard\QrFiles	Folder where query result files are written
ForwardedHeaders:KnownProxies	IP address of the load balancer	If the product is behind a reverse proxy. Only the X-Forwarded-For header from these addresses is processed and the real client IP is written to the audit trail. If the list is empty the header is not read
Evidence:Signing:Enabled	true	Evidence signing. The code default is false: while it is off, evidence files and packages are produced unsigned and nothing runs on a Production server (Section 4.4)
Evidence:Signing:InstallationId	COMPANY-PROD-01	Installation ID. Unique per installation, never changed later
Evidence:Signing:Keys:1:PublicKeyPem	Content of pub.pem	Section 2.3. Can be left empty when the certificate store is used
Evidence:Signing:Keys:1:CertificateThumbprint	Thumbprint of the certificate	Recommended: the signing key in the Windows certificate store (section 2.3)
Evidence:Ledger:DigestOutputPath	\\worm.company.local\changeguard-digest	Immutable store for the signed ledger digests. The path is seen from the API server (section 12.7)

Setting	Value to write at installation	Notes
Evidence:Ledger:DigestIntervalMinutes	60	Ledger digest interval
Evidence:Ledger:BoundaryCheckMinutes	15	Evidence write boundary check interval
Evidence:Ledger:DigestStaleAfterIntervals	2	If no digest arrives for this many intervals, Governance Readiness warns
Database:EvidenceLedger	true	The evidence table is created as a ledger. Not changed in production
Evidence:Signing:AllowUnsignedProductionExecution	false	While signing is off or the approval chain is unsigned, nothing runs on a Production server. true is only a deliberate exception; turning it on is recorded as App.ControlRelaxed (section 4.4)
Sandbox:AllowOnProduction	false	The sandbox does not run on a Production server. A sandbox runs an unapproved script on the target and rolls it back; COMMIT, linked server calls and sequence changes cannot be rolled back
Evidence:Signing:Keys:N:RevokedAt	Empty	The moment the key was revoked. Signatures made with that key after this moment count as invalid (section 12.4)

4.2 Email

Setting	Values	Notes
Mail:Enabled	true, false	When false, no email is sent
Mail:SmtpHost, Mail:SmtpPort	smtp.company.local, 587	SMTP server

Setting	Values	Notes
Mail:Username	Sender account	Its password is in the Mail__Password environment variable
Mail:FromAddress, Mail:FromName	changeguard@company.com, SQL Change Guard	Sender
Mail:EnableSsl	true, false	When true, the connection uses the encryption the server offers: encrypted from the start on port 465, and on other ports encrypted when the server offers STARTTLS. When false, no encryption is used
Mail:DevMode	false	false in production

Verification: the Settings > Diagnostics > Mail Test screen sends a test email with the same settings.

4.3 Timestamp (optional)

The digest of evidence dossiers is signed by an RFC 3161 timestamp server. Only the SHA-256 digest of the content is sent to the server; evidence content never leaves the organisation.

Setting	Values	Notes
Evidence:Timestamp:Mode	Off (default), On	Master switch. When Off, no network call is made
Evidence:Timestamp:Url	https://tsa.company.local/tsr	Address of the organisation's or a contracted authority
Evidence:Timestamp:TimeoutSeconds	10	Timeout
Evidence:Timestamp:ProxyUrl	http://proxy.company.local:8080	If empty, the operating system's configured proxy is used
Evidence:Timestamp:ProxyUseDefaultCredentials	true, false	true if the proxy expects the service's Windows identity
Evidence:Timestamp:ProxyBypass	tsa.company.local	Addresses that do not go through the proxy, separated by ;

If the server cannot be reached, work does not stop: the document is produced without a timestamp and a warning is written to the log. The connection is tested on the Settings > Diagnostics > Timestamp Test screen.

4.4 Approval chain and governance state

The product links the saved, the approved and the executed content of a request with signed events and checks before execution that they are the same. This chain shows that the product accepted and recorded the events; on its own it does not prove what happened on the target database. What to know at installation:

- Signing must be on. Evidence:Signing:Enabled = true (code default false) with a usable key (section 2.3). While signing is off, nothing runs on a Production server; Evidence:Signing:AllowUnsignedProductionExecution is the deliberate exception to this rule and stays false.
- The baseline is written at the first start. When the API starts for the first time it seals once the current state of the approval policies, the settings that affect approval, the never-skip standards and the user roles (Governance.StateSealed). The correctness of this state is the responsibility of the person who installs the product and is written in the installation record. Every later change is made from the product screens and is sealed again.
- If the tables are changed outside the application, no new approval plan is produced, a user whose role was changed cannot approve, and the event goes to the SOC as an alert. The state is shown on the "Approval policies and roles match the last sealed state" row of the Governance Readiness screen. After the difference has been reviewed, only a user with the SystemManager role accepts the state of the tables with the Rebaseline button on the same row, writing a reason (Governance.Rebaselined).
- The certificate of the target server should be validated. When "Validate the server certificate" is on in the server definition, the connection is validated against the certificate authority the organisation trusts. When it is off, the connection is encrypted but the identity of the target is not checked. It is recommended for Production servers; before switching it on, the certificate authority of the organisation is added as trusted on the API and Worker servers. On Oracle, validation is done with TCPS and server name matching.

5. Worker installation

1. The delivered Worker folder is copied to the server (for example D:\SQLChangeGuard\worker).
2. In the Worker folder's appsettings.json, the API address is written to WorkerApi:BaseUrl (for example https://changeguard-api.company.local). WorkerApi:Key is not left in the file; it is given with the WorkerApi__Key environment variable.

3. The service is registered (in a command prompt opened as administrator):

```
sc.exe create "ChangeGuardWorker" binPath= "D:\SQLChangeGuard\worker\SCG.Workers.exe" start=
auto DisplayName= "SQL Change Guard Worker"
```

```
sc.exe start "ChangeGuardWorker"
```

4. The service account is given write permission on the logs folder in the Worker folder and on the query result file folder. The Worker does not access the evidence signing key or the ledger digest folder; both are the work of the API. If the signing key is in the certificate store, read permission on the private key of the certificate is given to the API application pool identity.

5. Log file: logs\scg-worker-YYYYMMDD.log in the Worker folder. At start-up a Worker configuration loaded from API line is shown.

6. Database account: by default the Worker uses the same account as the API and the connection string comes from the API. For a separate account, define the ConnectionStrings__Worker environment variable on the Worker server (permissions in section 3.5). The source in use is written at start-up in the "Worker database connection source" line.

The Worker's job intervals are in the Workers section of the API's appsettings.json and reach the Worker through the API. The values in the table are the values in the delivered settings file and suit most organisations. MainWorkSeconds and ConnectionCheckSeconds have no default in code; do not remove these lines from the file:

Setting	Delivered value	Purpose
Workers:MainWorkSeconds	30	How often queued and due executions are picked up
Workers:ConnectionCheckSeconds	60	Interval of the target server connection check
Workers:ConnectionCheckFailureThreshold	3	Consecutive failed checks before a warning email for a server
Workers:StaleExecutionRecoveryMinutes	120	An execution claimed for longer than this is considered dead. Because the target may have committed, it is not run again and moves to Reconciliation Required; if it is certain that nothing was done on the target (the

Setting	Delivered value	Purpose
		execution failed and was rolled back), it returns to Approved. Must be longer than the longest legitimate execution
Workers:WorkerErrorMailTo	IT team address	Address that receives Worker errors
Workers:SiemPumpSeconds	10	Poll interval of SIEM delivery (section 10)
Workers:DirectorySyncPollSeconds	300	How often the Worker asks whether directory sync is due (section 7)
Workers:ItsmPumpSeconds	30	How often pending notes are sent to ITSM (section 9)

6. Web interface, licence and first sign-in

6.1 Web interface

1. The delivered web interface folder is copied to the server. The package is prepared with the organisation's API address.
2. A separate site is created in IIS with this folder as its root. An HTTPS binding is defined for the web interface address.
3. The web.config file in the folder redirects the request to index.html when a page is refreshed or a link in an email is opened. This needs the IIS URL Rewrite module.
4. The web interface address must be in the API's AllowedOrigins setting.

6.2 Licence

1. Sign in with the administrator account created by the installation (6.3).
2. Upload the content of the licence file on the Settings > License screen.
3. The product verifies the signature. An invalid file is not saved and does not break the working licence. The licence is stored in the database; the API and the Worker read the same record. Every licence change is written to the audit trail as a License.Activated event.

When License:ExpiryWarningDays (default 30) days are left, a warning appears in the interface. Renewal is done on the same screen.

6.3 First sign-in

If there are no users, the installation creates an administrator account: user name admin, password admin123. This account must change its password at first sign-in; that session is good for nothing else. Then:

1. Target servers are defined on the Servers screen.
2. Users are added, or the corporate directory or corporate sign-in is set up (sections 7 and 8).
3. Approval policies and parameters are set according to the organisation's rules.
4. The Settings > Diagnostics > Governance Readiness screen is opened and section 11 is applied.

Even when the corporate directory or corporate sign-in is used, at least one local SystemManager account is kept as a break-glass account. If the directory or the identity provider fails, the system is entered with this account.

7. Corporate directory (LDAP / Active Directory)

7.1 How it works

A person types the corporate user name and password on the product's sign-in screen. The product does not store the password; it asks the directory over an encrypted connection. If the password is correct, it reads the person's email, immutable identifier, account state and groups. It compares the groups with the role mapping table and assigns a role.

Who is asked in the directory:

- Users whose account type is LDAP.
- When Auth:Mode = Ldap, people who have no record in the product at all. If they are authenticated, their account is created (7.4).
- Local and SSO accounts are not asked in the directory.

Whether it is on or off depends on the Ldap:Host setting: if empty, the directory is not used.

7.2 Settings (appsettings.json, Ldap section)

Setting	Values	What to write
Host	Server name, without scheme	dc01.company.local. Empty = directory off
Port	Number	636 for Ldaps, 389 for StartTls. If not written these defaults are used
Security	Ldaps (default), StartTls, None	Ldaps is recommended. With None the password travels in clear text on the network; for tests only
AllowUntrustedCertificate	true, false	false in production. When true the directory certificate is not validated
BindFormat	DownLevel, Upn, SearchDn	For Active Directory DownLevel (COMPANY\user) or Upn (user@company.local). SearchDn for directories such as OpenLDAP
Domain	NetBIOS domain name	COMPANY. Required for DownLevel. If a person types a different domain, the password is not tried
UpnSuffix	UPN suffix	company.local. Required for Upn
BaseDn	Directory path	DC=company,DC=local or OU=Staff,DC=company,DC=local. Required. People outside this path are not found
UserFilter	LDAP filter	Active Directory: {&(objectClass=user)(sAMAccountName={user})}

Setting	Values	What to write
		{user} is replaced by the typed name. Must return exactly one person
BindDn	Full name of the service account	CN=changeloguard-reader,OU=Service,DC=company,DC=local. Required for the SearchDn format and for sync. Its password is in the Ldap__BindPassword environment variable
IdentityAttribute	objectGUID (default), entryUUID	Active Directory: objectGUID. OpenLDAP: entryUUID. Never changed after installation
EmailAttribute	Default mail	No account is created for a person without an email in the directory
DisplayNameAttribute	Default displayName	Display name
GroupMatch	Dn (default), Cn	Dn is recommended: the group is compared by its full name. With Cn, groups with the same name in different folders are not told apart
NestedGroups	true (default), false	When true, nested groups also count (up to 10 levels, 500 groups)
RoleSource	Manual (default), Directory	7.4
TimeoutSeconds	2 to 60, default 10	Timeout of a directory call
Sync:Enabled	true, false (default)	true is recommended in production (7.5)
Sync:IntervalMinutes	15 to 1440, default 60	Minimum time between two syncs
Sync:AbortRatio	Default 0.2	Safety limit (7.5)
Sync:AbortMinCount	Default 5	Safety limit (7.5)

Related Auth setting: with Auth:Mode = Local (default) only accounts created in the product can sign in. With Ldap, a person without a record in the product is asked in the directory.

Active Directory example:

```
"Ldap": {
  "Host": "dc01.company.local",
  "Port": 636,
  "Security": "Ldaps",
  "AllowUntrustedCertificate": false,
  "BindFormat": "DownLevel",
  "Domain": "COMPANY",
```

```

"BaseDn": "DC=company,DC=local",
"UserFilter": "(&(objectClass=user)(sAMAccountName={user}))",
"BindDn": "CN=changeguard-reader,OU=Service,DC=company,DC=local",
"IdentityAttribute": "objectGUID",
"GroupMatch": "Dn",
"NestedGroups": true,
"RoleSource": "Directory",
"Sync": { "Enabled": true, "IntervalMinutes": 60, "AbortRatio": 0.2, "AbortMinCount": 5 }
}

```

7.3 What is read from the directory and where it is written

Directory attribute	Where it is written in the product	Notes
sAMAccountName	Users.DomainUsername	User name of a new account. If the attribute is missing, the name the person typed is used
mail (EmailAttribute)	Users.Email	Updated at every sign-in and sync
objectGUID or entryUUID (IdentityAttribute)	UserExternalIdentities.Subject (Provider = Ldap)	Immutable identifier. The account is bound to it at first sign-in; even if the user name changes or a new person arrives with the same name, the account does not pass to the wrong person
memberOf (including nested)	Users.Role (through the mapping table)	The role is calculated (7.4)
userAccountControl	Not stored	If the account is disabled (Active Directory ACCOUNTDISABLE bit), sign-in is rejected and sync removes access
lockoutThreshold (at the domain root)	Not stored	The directory's lockout threshold. Compared with the product's threshold on the Governance Readiness screen

A new directory account is written to the Users table with AuthType = Ldap and an empty password hash. The password of a directory account cannot be reset in the product.

7.4 Group to role mapping

Mappings are defined on the Settings > Corporate Identity (SSO and LDAP) screen by choosing the "Directory (LDAP)" provider. Each row binds a group to a role:

Provider	Value	Role
Directory (LDAP)	CN=DBA-Team,OU=Groups,DC=company,DC=local	DbAdmin
Directory (LDAP)	CN=Change-Board,OU=Groups,DC=company,DC=local	ChangeManager
Directory (LDAP)	CN=Requesters,OU=Groups,DC=company,DC=local	Requester

Rules:

- If several groups match, the highest role is given.
- SystemManager is never given through a mapping; it is given only by hand on the Users screen.
- Spaces and letter case in the value do not matter.
- If you do not know the value, let the person try to sign in once. The ReceivedGroups field of the LdapLoginDenied record in Audit Logs lists the groups that came from the directory.
- A mapping change is written to the audit trail; if settings approval is on, it goes through a second administrator's approval.

Source of the role (Ldap:RoleSource):

	Manual (default)	Directory
New person at first sign-in	Created with the mapped role; without a mapped group, created with no access (NoAccess) and an administrator gives the role	Created with the mapped role; without a mapped group the account is not created
Role of an existing person	Whatever the administrator gave	Recalculated from the groups at every sign-in and sync
Role on the Users screen	Changes by hand	Does not change (only SystemManager can be given and taken back)
If groups cannot be read	A new account is not created	The existing role is not lowered; sign-in is rejected

7.5 Synchronisation

When sync is on, the Worker periodically asks the API whether sync is due; the API performs the sync. All directory accounts of the product are looked up in the directory with the service account:

State in the directory	What happens in the product
Person not found or account disabled	Role becomes NoAccess, open sessions are closed. The account is not deleted
Group changed (in Directory mode)	Role is recalculated; if it changed, sessions are closed
Email changed	Updated

Safety limit: if the number of accounts to be closed in one sync is not lower than AbortMinCount and the ratio exceeds AbortRatio, the sync makes no change and writes an Ldap.SyncAborted event. It exists so that a wrong BaseDn or a temporary problem in the directory does not lock everyone out. If the directory cannot be reached, no change is made either. The last SystemManager account that can manage the system is never closed.

The Synchronise now button on the Settings > Corporate Identity (SSO and LDAP) screen works even when sync is off.

7.6 Lockout threshold

The product counts wrong passwords and locks the account after Auth:AccountLockoutMaxAttempts attempts. The directory has its own threshold. The product's threshold must be lower than the directory's; otherwise someone could lock a person's corporate account by guessing passwords on the product's screen. For names that have no account in the product, after Auth:AccountLockoutMaxAttempts wrong attempts for the same name the directory is not asked for Auth:AccountLockoutMinutes minutes.

7.7 Installation order

1. A read-only service account is obtained from the directory team; its password is written to the Ldap__BindPassword environment variable.
2. Check that the root certificate that issued the directory certificate is trusted on the API server.
3. The Ldap section is filled in and the API is restarted.
4. On the Settings > Corporate Identity (SSO and LDAP) screen, press Test connection. If it fails, the step is shown: configuration, connecting to the server, signing in with the service account or reading BaseDn.
5. Role mappings are defined; then, if needed, RoleSource = Directory and Auth:Mode = Ldap are set.
6. Synchronise now is run; the directory rows on the Governance Readiness screen are checked.

Every later change in this section is detected at API start-up and written to the audit trail with its old and new values as an Ldap.ConfigurationChanged event. The password is not written.

8. Corporate sign-in (SSO)

8.1 How it works

A person presses the corporate sign-in button on the sign-in screen. The browser goes to the organisation's identity provider; the password and MFA are entered there and never reach the product. The identity provider sends the person back to the product with a signed identity assertion. The product checks the signature, who issued it, for whom it was issued, its validity period and whether it belongs to its own request. It finds or creates the person by the immutable identifier, maps the group to a role and opens its own session.

Supported protocols: OIDC (Microsoft Entra ID, Keycloak, Okta) and SAML 2.0 (AD FS, Entra ID, Keycloak). Several identity providers can be defined at the same time; each is a separate button on the sign-in screen. LDAP and SSO can be on at the same time; each account signs in with its own type.

8.2 General settings (appsettings.json, Sso section)

Setting	Values	What to write
Enabled	true, false (default)	When false SSO is off; open sessions of SSO accounts also end when the API restarts. This is the emergency switch if the identity provider is suspected
ApiBaseUrl	The API address as seen from the browser	https://change-guard-api.company.local. Return addresses are built from it, never derived from the request
FrontendBaseUrl	Address of the web interface	https://change-guard.company.local
AutoProvision	true (default), false	When true, a person without an account is created at first sign-in. When false, the administrator creates the account beforehand with the "Corporate account" type
RoleSource	Idp (recommended), Manual	Idp: the role is recalculated from the groups at every sign-in. Manual: the group gives the role only when the account is first created
MaxSessionHours	Hours, 0 = no limit	The smaller of this and Auth:MaxSessionHours applies. The session of an account disabled at the identity provider ends at the latest after this time

Setting	Values	What to write
SignOutFromIdp	true, false	When true, signing out of the product also signs out of the identity provider (OIDC only)
LoginTimeoutMinutes	1 to 60, default 10	Time allowed to return from the identity provider
ExchangeCodeSeconds	30 to 600, default 120	Lifetime of the single-use code after the return
ClockSkewMinutes	0 to 15, default 5	Accepted difference between server clocks

Related Auth setting: only break-glass accounts are written to Auth:LocalLoginAllowedUsers (for example ["admin"]). When the list is not empty, only the local accounts in it can sign in with a password. While SSO is on, every sign-in with these accounts is written to the audit trail as a LoginBreakGlass event and goes to the SOC as an alarm.

8.3 Identity provider settings (Sso:Providers list)

Setting	OIDC	SAML
Name	Permanent name, for example Entra. Letters, digits, - and _ (up to 50). Never changed after installation: user links and mappings are kept under this name	Same
DisplayName	Name shown on the button	Same
Protocol	Oidc	Saml
RequireHttpsMetadata	true in production	true in production
Authority	Entra ID: https://login.microsoftonline.com/tenant-id/v2.0 . Keycloak: https://server/realms/realms	Not used
ClientId	Client ID of the application registration	Not used
ClientSecret	Empty in the file; Sso__Providers__N__ClientSecret	Not used
Scopes	Default profile, email	Not used
IdpMetadataUrl	Not used	AD FS: https://adfs/FederationMetadata/2007-06/FederationMetadata.xml

Setting	OIDC	SAML
SpEntityId	Not used	If empty, {ApiBaseUrl}/api/auth/sso/saml/metadata/{Name}
SpCertificatePath, SignAuthnRequests	Not used	If the identity provider requires signed requests, the .pfx path and true. Its password is Sso__Providers__N__SpCertificatePassword
SubjectClaim	Entra ID: oid. Keycloak, Okta: sub	NameID (must be persistent)
UsernameClaim	preferred_username	AD FS: http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn
EmailClaim	email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress
GroupsClaim	Entra ID: roles (recommended) or groups. Keycloak: groups	http://schemas.microsoft.com/ws/2008/06/identity/claims/role
RequireMfaClaim	true in production	true in production
MfaClaim, MfaClaimValue	amr, mfa	AuthnContextClassRef, http://schemas.microsoft.com/claims/multipleauthn

8.4 What is read from the assertion and where it is written

Field in the assertion	Setting	Where it is written in the product
Immutable identifier (oid, sub, NameID)	SubjectClaim	UserExternalIdentities.Subject. The provider's Name is written to the Provider column. The person is found by this at later sign-ins
User name	UsernameClaim	Users.DomainUsername. Used only for a new account and for the first link to a pre-created SSO account; it does not change afterwards
Email	EmailClaim	Users.Email. Required for a new account; updated at every sign-in
Groups or roles	GroupsClaim	Users.Role (through the mapping table)
MFA information	MfaClaim, MfaClaimValue	Not stored. When RequireMfaClaim is true and the value is missing, sign-in is rejected. The MFA information of the session in which a decision was made goes into the evidence dossier

A new SSO account is written to the Users table with AuthType = Sso, an empty password and an empty MFA secret. MFA is done by the identity provider.

8.5 Group to role mapping

Mappings are defined on the Settings > Corporate Identity (SSO and LDAP) screen by choosing the provider's name. The Value field holds the text that arrives in the assertion:

Identity provider	Value that arrives	Example mapping value
Entra ID, application role (recommended)	The role value defined in the application registration	ChangeGuard.DbAdmin
Entra ID, group	Not the group name but its ID (Object ID)	5f3c1a2e-8b0d-4e6f-9a17-2c4d8e9f0a11
AD FS	Group name, according to the claim rule	DBA-Team
Keycloak	Group name	dba-team

The rules are the same as for LDAP: the highest role wins, SystemManager is never given through a mapping, and if you do not know the value, look at the ReceivedGroups field of the SsoLoginDenied record in Audit Logs. With RoleSource = Idp, when a mapping is changed or deleted, the open sessions of people linked to that provider with that role are closed immediately.

8.6 What to do at the identity provider

The Settings > Corporate Identity (SSO and LDAP) screen shows the addresses to enter at the identity provider, ready to copy: Redirect URI, Post sign-out redirect URI, and for SAML the Application identifier (Entity ID), Reply address (ACS) and Application metadata.

Microsoft Entra ID (OIDC):

1. App registrations > New registration. Redirect URI (Web): the Redirect URI on the screen.
2. Certificates & secrets > New client secret. The value is written to the Sso__Providers__N__ClientSecret environment variable.
3. App roles: one value for each product role (for example ChangeGuard.DbAdmin). Assigned to users or groups under Enterprise applications.
4. Token configuration > Add optional claim > ID > email.
5. appsettings: Authority, ClientId, SubjectClaim = oid, GroupsClaim = roles, RequireMfaClaim = true, MfaClaim = amr, MfaClaimValue = mfa, RequireHttpsMetadata = true.

AD FS (SAML):

1. Relying Party Trusts > Add. Give the Application metadata address on the screen (or upload it as a file).
2. Claim issuance policy: NameID (Persistent), UPN, E-Mail Address, Role.

3. appsettings: Protocol = Saml, IdpMetadataUrl, UsernameClaim, EmailClaim, GroupsClaim and MfaClaim with the values in 8.3.

8.7 Installation order

1. The application registration is made at the identity provider (8.6); the secret is written to an environment variable.
2. The Sso section is filled in, Enabled = true is set and the API is restarted.
3. On the Settings > Corporate Identity (SSO and LDAP) screen, the provider's Test connection button shows that the metadata is read.
4. Role mappings are defined.
5. Sign in with a test user; in the SsoLoginSuccess record in Audit Logs, check that the role and the MFA information arrive as expected.
6. Auth:LocalLoginAllowedUsers is filled with break-glass accounts only.

Every later change in this section and in the Auth:LocalLoginAllowedUsers list is detected at API start-up and written to the audit trail with its old and new values as an Sso.ConfigurationChanged event. Secrets are not written.

9. ITSM integration

9.1 How it works

ITSM (ServiceNow, Jira Service Management, ServiceCore) keeps the organisation's work records: change records, incidents, service requests. ITSM answers "should this work be done, did the CAB allow it"; SQL Change Guard answers "exactly which script, on which server, who approved it, who ran it". The integration links the two. When ITSM is on, the product:

1. When a request is saved, checks that the number exists in ITSM, is of the right kind and is not closed.
2. Right before execution (the Execute button, scheduled execution, release package and the Worker's final check), checks that the record is implementable. This check does not use a cache.
3. When scheduling, blocks what will certainly stop at that time and warns about what is not yet known.
4. Keeps what it saw in ITSM as evidence.
5. Writes the important steps of the request to the ITSM record as notes.

The product does not change the state of the ITSM record, does not close it and does not delete it. No script text, result data or password is written into a note.

ITSM counterparts of our request types:

Request	ITSM record	Field on the screen (ITSM on)
Change	Change record (for example CHG0030001)	Change record no
Query result (data extraction)	Service request (for example RITM0010001). Can be set to Change or None with ItsmQueryResultTicketKind	Service request no
Rollback	The change record of the source request	Comes from the source
Request marked Emergency	In addition, an incident (for example INC0012345)	Incident no

The kind of a number is decided by the field it is typed in; the product does not guess the kind from the number.

9.2 Connection settings (appsettings.json, Itsm section)

This section holds only the connection. The switch that turns ITSM on and off is the ItsmEnabled parameter in the product (9.6).

Setting	Values	What to write
Provider	None, ServiceNow, Jira, GenericRest	GenericRest: ServiceCore and any ITSM not in the list
BaseUrl	Address, without a trailing /	ServiceNow: https://company.service-now.com. Jira Cloud: https://company.atlassian.net. Jira Data Center: https://jira.company.local
AuthType	Basic, Bearer, HeaderKey	ServiceNow and Jira Cloud: Basic. Jira Data Center: Bearer. An ITSM that wants an API key in a header: HeaderKey
Username	Integration account	On Jira Cloud, the account's email
Password	Empty in the file; Itsm__Password	Password for Basic. On Jira Cloud, the API token
Token	Empty in the file; Itsm__Token	Key for Bearer and HeaderKey
HeaderName	Header name	For HeaderKey only, for example X-API-Key
Proxy	Proxy address	If a cloud ITSM is reached through a proxy, for example http://proxy.company.local:8080
TimeoutSeconds	2 to 60, default 10	When exceeded, ITSM is considered unreachable
CacheSeconds	0 to 600, default 60	Cache of lookups on the request screen. The execution check does not use a cache
AllowUntrustedCertificate	true, false	false in production
ProductBaseUrl	Address of the web interface	Root of the link added at the end of an ITSM note, for example https://changeloguard.company.local. If empty, the note has no link

The integration account gets the least permission. ServiceNow: read on the change_request, incident and sc_req_item tables, write to the work_notes field. Jira: browse and add comments in the relevant projects. No permission to change states or delete.

9.3 ServiceNow: what is read and where it is written

The product looks up each record kind in its own table. The tables can be changed under Itsm:ServiceNow:

Setting	Default	Record kind
ChangeTable	change_request	Change record
IncidentTable	incident	Incident
RequestTable	sc_req_item	Service request

Lookup: GET

{BaseUrl}/api/now/table/{table}?sysparm_query=number={number}&sysparm_limit=1&sysparm_display_value=all. Writing a note: PATCH {BaseUrl}/api/now/table/{table}/{sys_id}, with work_notes in the body.

ServiceNow field	Part read	In the product (ItsmTickets table)
number	Displayed value	TicketNo
short_description	Displayed value	Title
state	Displayed name (for example Implement, Authorize, Closed)	ExternalState
approval	Displayed name (for example Approved, Requested)	Approval. Evaluated as approval only for change records
start_date	UTC internal value	PlannedStart
end_date	UTC internal value	PlannedEnd
sys_id	Internal value	Not stored. Used for writing notes and for the link: Link = {BaseUrl}/table.do?sys_id={sys_id}
(calculated by the product)		StateClass (9.5), Source = ServiceNow, LastVerifiedAt = time of the lookup

If the record is not found, ServiceNow returns an empty list and the product reports "not found". If a number is typed in the wrong field (for example an incident number in the change field), the result is "not found", because that number is not in the change table.

9.4 Jira and other ITSMs: what is read and where it is written

Jira (Itsm:Jira):

Setting	Example	Purpose
ApiVersion	2 (Cloud and Data Center), 3 (Cloud only)	With 3, the note body is sent in Atlassian Document Format

Setting	Example	Purpose
ChangeIssueTypes	Change	Type names treated as change records, separated by ;. If empty, the type is not checked
IncidentIssueTypes	Incident	Incident types
RequestIssueTypes	Service Request;Service Request with Approvals	Service request types
PlannedStartField, PlannedEndField	customfield_10050, customfield_10051	IDs of the planned start and end custom fields. Found with GET /rest/api/2/field. If empty, the planned window is not read

Lookup: GET {BaseUrl}/rest/api/{version}/issue/{key}?fields=summary,status,issuetype plus the planned fields. Note: POST {BaseUrl}/rest/api/{version}/issue/{key}/comment.

Jira field	In the product
key	TicketNo
fields.summary	Title
fields.status.name	ExternalState
fields.status.statusCategory.key (new, indeterminate, done)	Not stored. Every state in the done category counts as closed
fields.issuetype.name	Not stored. If it is not in the expected type list, "wrong kind"
PlannedStartField, PlannedEndField	PlannedStart, PlannedEnd
(approval)	No separate approval field is read in Jira; approval is expressed by the workflow state (ItsmReadyStates). Approval stays empty
(calculated by the product)	Link = {BaseUrl}/browse/{key}, StateClass, Source = Jira

ServiceCore and others (Itsm:GenericRest). Without code changes, the ITSM's API address and the path of each field in the response are written. A path is separated by dots, with a number for an array (for example result.0.state):

Setting	What to write	In the product
ChangeUrlTemplate, IncidentUrlTemplate, RequestUrlTemplate	The address that reads a record; {ticket} is replaced by the number	
StatePath	Path of the state field (required)	ExternalState

Setting	What to write	In the product
StateCategoryPath	Path of the state category field (optional)	If the value is done, the record counts as closed
TitlePath	Path of the title field	Title
ApprovalPath	Path of the approval field. When set, approval is required for change records	Approval
PlannedStartPath, PlannedEndPath	Paths of the planned time fields	PlannedStart, PlannedEnd
TypePath and ChangeTypes, IncidentTypes, RequestTypes	Path of the type field and the type names of each kind	If the type is not in the expected list, "wrong kind"
IdPath	Internal ID of the record	Not stored
BrowseUrlTemplate	Address that opens the record in a browser	Link
CommentUrlTemplate, CommentMethod, CommentBodyTemplate	Note address ({ticket}, {kind} = change, incident or request), POST or PUT, JSON body ({message} and {ticket} are inserted)	

If both the state and title fields are empty, or ITSM returns 404, the record counts as not found.

9.5 How the state is interpreted (StateClass)

State names in ITSM differ between organisations. The product classifies the state with three parameters. Letter case and leading or trailing spaces do not matter in comparisons. The rules are applied in order; the first match wins:

Order	Condition	StateClass
1	State is empty	Unknown
2	State is in ItsmClosedStates	Closed
3	State category is done (Jira or StateCategoryPath)	Closed
4	The record is not a change record (incident, service request)	Open
5	State is in ItsmReadyStates and approval is not read from a separate field (Jira; GenericRest with empty ApprovalPath)	Ready
6	State is in ItsmReadyStates, approval is read but arrived empty	Unknown

Order	Condition	StateClass
7	State is in ItsmReadyStates, approval is in ItsmApprovedValues	Ready
8	State is in ItsmReadyStates, approval has another value	Pending
9	Any other state	Pending

Effect of the class on decisions:

StateClass	On save (ItsmVerifyOnSave = Block)	On execution (ItsmExecuteGate = Block)
Ready	Saved	Runs. With ItsmEnforceWindow = true it must also be inside the planned window now
Pending	Saved (a request can be prepared before the CAB)	Stops for a change record: no CAB approval or the record is not ready
Unknown	Saved	Stops for a change record
Open	Saved	Runs for service requests and incidents (they have no CAB approval)
Closed	Not saved	Stops

ServiceNow change record example (with default parameters):

state	approval	StateClass	Result
Authorize	Requested	Pending	Saved, not executed
Implement	Approved	Ready	Executed
Implement	(empty)	Unknown	Not executed, because the approval could not be read
Closed	Approved	Closed	Not saved, not executed

A stopped request is not rejected: it waits in the Approved state and is executed again when the ITSM record becomes suitable. If a scheduled execution stops, the schedule is cleared and an email goes to the requester and the approvers. If a request in a release package stops, the package does not start at all.

Exceptions:

- A rollback linked to its source is exempt from the execution and scheduling checks. After the source is applied the ITSM record is usually closed; if the rollback were blocked, something broken could not be fixed. The exemption is recorded.
- For an emergency request CAB approval is not required; a closed, missing or wrong-kind change record still stops it. The exemption is recorded.
- If ITSM cannot be reached, ItsmUnavailablePolicy decides. An emergency request always passes.

9.6 Behaviour parameters (Settings > Parameters > ITSM Ticket)

Parameter	Default	Values	Purpose
ItsmEnabled	false	true, false	Master switch. When false the product never contacts ITSM and writes no notes; numbers are checked only by the format and requirement rules
ItsmVerifyOnSave	Block	Block, Warn, Off	On save, if the number breaks the rule (closed, missing, wrong kind): reject, save with a warning, or do not ask at all
ItsmExecuteGate	Block	Block, Off	Whether ITSM is asked before execution. The scheduling check also depends on it
ItsmEnforceWindow	false	true, false	When true, work can run only inside the planned window in ITSM and cannot be scheduled outside it. If the record has no window, execution stops
ItsmVerifyIncident	Warn	Block, Warn, Off	What happens if the incident number of an

Parameter	Default	Values	Purpose
			emergency request is closed or missing
ItsmUnavailablePolicy	AllowAndRecord	AllowAndRecord, Block	If ITSM cannot be reached: continue and record it (an alarm goes to the SOC), or stop
ItsmQueryResultTicketKind	Request	Request, Change, None	Which kind of ITSM record the number of a query result request is. None: ITSM is not asked, only the format is checked
ItsmReadyStates	Scheduled;Implement	List separated by ;	A change record in these states counts as implementable
ItsmClosedStates	Review;Closed;Canceled;Cancelled;Resolved;Closed Complete;Closed Incomplete;Closed Skipped	List separated by ;	A record in these states counts as closed
ItsmApprovedValues	Approved	List separated by ;	Values in the approval field that count as approved
ItsmWriteBackEnabled	true	true, false	Whether notes are written to the ITSM record
ItsmWriteBackEvents	List of request steps	Event names separated by ;	Which steps are sent as notes (created, approved, scheduled, executed, failed, stopped by the ITSM check)

Number rules. They apply when ITSM is off too:

Parameter	Default	Purpose
ChangeTicketRequired	Always	Whether the main field is required: Always, ExceptEmergency, Never

Parameter	Default	Purpose
EmergencyTicketRequired	Never	Whether the incident number is required on an emergency request: Always, Never
ChangeTicketRegex	^CHG\d{7}\$	Format of the change record number
RequestTicketRegex	^RITM\d{7}\$	Format of the service request number. If left empty, ChangeTicketRegex also applies to query result requests
EmergencyTicketRegex	^INC\d{7}\$	Format of the incident number

The product does not accept invalid values: a misspelled value, an empty state list or a regex that does not compile is not saved. These are control parameters: a change is written to the audit trail and goes into the rule set frozen on the request when it is saved. In addition, the record of every ITSM decision carries the rule values that made the decision; they are shown under each decision in the evidence dossier.

9.7 The note written to ITSM

Example:

SQL Change Guard #7: executed successfully. Server: SQLPROD01. By: WorkerService (started by ayse.dba), 28.09.2026 02:09 Europe/Istanbul (UTC+03:00). Risk band: Medium. Details: <https://change-guard.company.local/change-requests/7>

The Worker writes the execution result; the person who started the execution is shown in brackets (started by).

Notes are sent by the API at the Worker's request (Workers:ItsmPumpSeconds). If ITSM cannot be reached, a note is not lost; it is sent in order when ITSM recovers. If notes cannot be sent for 15 minutes, an Itsm.WriteBackStalled event is written once.

9.8 Installation order

1. The connection is written to the Itsm section, the secret is put in an environment variable and the API is restarted.
2. On the Settings > ITSM screen, the Test connection button looks up a real change record; check that the state is interpreted correctly.
3. ItsmReadyStates, ItsmClosedStates and, if needed, ItsmApprovedValues are adjusted to the organisation's state names.
4. The number formats are set to the organisation's formats.
5. Decide what query result requests are based on (ItsmQueryResultTicketKind).

6. Set ItsmEnabled = true.

7. Check that no red row remains in the ITSM integration group of the Governance Readiness screen.

Every later change in the Itsm section is detected at API start-up and written to the audit trail as an Itsm.ConfigurationChanged event. Secrets are not written.

10. SIEM / SOC integration

10.1 How it works

The product sends governance events to the organisation's SOC collector over syslog. The sender in the Worker wakes up every ten seconds by default (immediately for records the Worker itself writes), converts the records after the delivery mark to the selected format, sends them and advances its "sent up to here" mark. If sending fails, the mark does not advance and the next cycle continues from the same place. Audit and ledger digest events are not lost on the product side; delivery is at least once, and the SOC removes duplicates by event ID. Over UDP, receipt by the collector cannot be confirmed.

There are four streams:

Stream	Content	Loss
Audit	Audit records	None
Anchor	Ledger digest events (published, failed, restore, fork)	None
AppLog	The product's own warning and error log	Possible: when the memory queue is full the oldest entry is dropped; the count is shown in the heartbeat
Heartbeat	Sign of life (every 5 minutes by default)	Tells "no events" apart from "product stopped"

10.2 Connection settings (appsettings.json, Siem section)

Several endpoints can be defined; each keeps its own mark.

Setting	Values	What to write
Endpoints[].Name	Endpoint name	SOC. Never changed after installation: if it changes, the endpoint counts as new and all past events are sent again
Endpoints[].Type	Syslog, File	Syslog is the real target. File writes one event per line (organisations without a collector, acceptance tests)
Endpoints[].Host, Port	Collector	siem.company.local, 6514
Endpoints[].Protocol	Tls (default), Tcp, Udp	Tls is recommended. UDP loses a message that does not fit in one packet and does not say so

Setting	Values	What to write
Endpoints[].Format	Rfc5424Json (default), Cef, Leef, Json, Rfc5424Sd	Cef for ArcSight, Leef for QRadar, Rfc5424Json for Splunk, Elastic and Graylog
Endpoints[].Facility	local0	Syslog facility
Endpoints[].TlsServerCertThumbprint	Thumbprint or empty	If empty, the system trust chain is used. If set, the server certificate is compared with it; on a mismatch the connection is refused and it never falls back to plain text
Endpoints[].FilePath	File path	Only for Type = File
Endpoints[].BatchSize	Default 200	Maximum events per cycle
Endpoints[].PollSeconds	Default 10	Poll interval. Records written by the Worker itself are sent immediately; records written by the API are sent within this interval (10 seconds by default)
Endpoints[].HeartbeatMinutes	Default 5	Heartbeat interval
AppLogQueueSize	Default 10000	Capacity of the memory queue for the product log
AppLogMinLevel	Default Warning	Product log entries below this level do not enter the queue

Worker side: Workers:SiemPumpSeconds (default 10) and Workers:SiemLeaseSeconds (default 60; with several Workers, a single writer per stream).

10.3 Behaviour parameters (Settings > Parameters > SIEM)

Parameter	Default	Values	Purpose
SiemEnabled	true	true, false	Master switch. It is on after installation; if no endpoint is defined in appsettings nothing can be sent, and this is shown on the Governance Readiness screen. When off, it is also shown as missing on the same screen
SiemStreams	Audit;Anchor;AppLog;Heartbeat	Separated by ;	Streams to send. If empty, all four are sent

Parameter	Default	Values	Purpose
SiemMinSeverity	Notice	Info, Notice, Warning, Error, Alert	Events below this threshold are not sent
SiemIncludeScriptText	false	true, false	Whether the full script text is sent. When off only the script digest is sent; a script may contain business data

Events not affected by the threshold: whatever SiemMinSeverity is, these events are sent: emergency actions (events whose name contains Emergency, Bypass or Override), permission denials and authentication failures, control weakening (approval policy, SQL standard, critical object, parameter, role, server, licence, settings change and SIEM setting events; user creation, deletion, role change and session revocation), attempts stopped by the approval chain gate (ChangeRequest.ApprovalBlocked, ChangeRequest.ExecutionBlocked, Worker.SealRejected, Governance.StateMismatch and release package blocks), evidence write boundary events (Evidence.BoundaryBroken, Evidence.BoundaryRestored), ledger digest events and the heartbeat. This rule applies to the severity threshold; if a stream is closed with SiemStreams, the events of that stream are not sent. The organisation can narrow the scope, but every narrowing is announced to the SOC with the old settings.

10.4 Event fields

Only fields that help classify the event are included. Script text (when SiemIncludeScriptText is off), result data, passwords and connection strings are never included. From the content of the audit record only these fields are carried: serverName, targetServer, databaseName, riskBand, riskScore, queryType, status, changeTicket, emergencyTicket, statementCount, objectCount, rowCount, maskedColumnCount, isEmergency, policyName, stepOrder, roleName, signingKeyId, mustChangePassword, reason, rejectionReason. Execution and sandbox window events also carry these fields for DAM matching: windowId, windowKind, windowOutcome, executionLogin, executorHost, clientAddress, observedLogin, observedDatabase, loginMismatch, targetSessionId, targetAuditSessionId, sessionApplicationName, executionStartedAt, executionFinishedAt, packageId, requestIds, sandboxId. The masking record event carries the servers, masked and unmasked column names, who approved the unmasking, the policy, the masking mode and counts; result data is not sent. Values that look like secrets are sent as *, and values longer than 256 characters are truncated. In the ledger digest event (Ledger.DigestPublished) these fields are carried: blockId, digestHash, digestTime, lastTransactionCommitTime, externalStore, file, envelopeSha256, signingKeyId, database. Because CEF has a limited number of free fields, the block number and the digest are carried first.

Information	Rfc5424Json and Json	Cef	Leef
Event ID (AuditLogs.Id)	eventId	externalId	externalId
Stream	stream	cat	stream

Information	Rfc5424Json and Json	Cef	Leef
Event name	action	Event class and name in the header	Event ID in the header
Record type	entityType	cs1 (entityType)	cat
Record ID	entityId	cs2 (entityId)	resource
User	user	suser	usrName
IP address	src	src	src
Severity	severity	Severity in the header	sev
Outcome	outcome (success, failure, unknown)	outcome	outcome
Time (UTC)	occurredAt	rt	devTime
The content fields above	Same names	Labelled fields cs3 to cs6 and cn1 to cn3	Same names

Severity mapping:

Product	Syslog	CEF and LEEF
Alert	1 (alert)	8
Error	3 (error)	6
Warning	4 (warning)	6
Notice	5 (notice)	4
Info	6 (informational)	1

The event id (eventId) links a record in the SOC to the audit record in the product; if the same event is sent again, the SOC can drop it by this id.

10.5 Installation order

1. The collector endpoint is written to the Siem section; the API and the Worker are restarted.
2. On the Settings > Diagnostics > SOC / SIEM screen, press Send test message. The test message goes through the same path as real events and carries Turkish characters; check that it looks right in the collector. The test works even while SiemEnabled is off.
3. Set SiemEnabled = true.
4. The last successful delivery and the delivery lag are watched on the same screen.

11. Installation verification

The Settings > Diagnostics > Governance Readiness screen shows live whether the installation is correct. Each row compares the current value of a setting with the expected value and states where the setting is made. The groups are: Segregation of duties, Rollback and isolated trial, Request discipline, Identity and passwords (including the corporate directory and corporate sign-in rows), Data protection, Audit and evidence (including the SOC / SIEM rows), ITSM integration, Secret placement and Verified outside the product. Each row's status is shown as In order, Attention or Decide.

1. Open the screen.
2. For every row marked Attention, decide: change the value, or record in the organisation's records why it was not changed.
3. Rows marked Decide have no single right answer; a conscious choice is enough.
4. When the installation is finished, a screenshot of the screen can be added to the installation acceptance record.

Other tests on the Diagnostics screen: Mail Test, Timestamp Test, SOC / SIEM. Corporate directory, corporate sign-in and ITSM connections are tested with the Test connection buttons on their own screens.

Short checklist:

- ☐ No errors in the API and Worker logs; the Worker received its configuration from the API at start-up
- ☐ The admin password has been changed; at least one local break-glass SystemManager account exists
- ☐ The licence is valid
- ☐ In the Secret placement group every secret comes from an environment variable
- ☐ Mail:DevMode is false, the test email arrived
- ☐ The "Evidence table is a ledger" and "Evidence write boundary" rows are green
- ☐ The ledger digest folder is defined; after the Worker started, the first digest file appeared in it
- ☐ The signing key is in the Windows certificate store
- ☐ The "Approval policies and roles match the last sealed state" row is green; the moment the baseline was written is in the installation record
- ☐ The "Unsigned execution on Production" and "Sandbox on Production servers" rows are green (both false)

- ☐ The "Certificate validation on Production servers" row is green, or the reason it is not switched on is in the organisation records
- ☐ The Governance Readiness rows of the integrations in use are green

12. Operations

12.1 Logs

Process	File	Notes
API	logs\scg-YYYYMMDD.log in the API folder	Rolls daily
Worker	logs\scg-worker-YYYYMMDD.log in the Worker folder	Rolls daily

Logs are in English. Warning and error entries also go to the SOC through the AppLog stream when SIEM is on.

12.2 Backup

- Application database: full and log backups with the organisation's standard plan.
- Keys: the Jwt, Security and evidence signing keys are backed up in the organisation's secret vault. If Security:ServerPasswordKey is lost, server passwords are entered again.
- Audit records (evidence.AuditLogs) are in a ledger table; the database engine rejects deleting and changing them. A restore on the same server is noticed from the msdb restore history and the Ledger.RestoreDetected event is written; a return behind the external digest shows up as Ledger.ForkDetected (12.7); the periods before and after the restore are verified with separate digest sets.
- Ledger digest folder: the immutable store of the organisation; its retention is longer than the database backups.

12.3 Upgrading

1. A new version may come with new installation scripts. Script names are in the release notes.
2. The API, Worker and web interface folders are replaced with the new ones; the appsettings.json files are kept.
3. With AutoMigrate = true the API applies the new scripts at start-up. With false the DBA applies the new scripts and runs the DbSchemaVersions.ps1 output; if a script is missing, the API names it and does not start.
4. The Worker service is restarted.

12.4 Changing keys

Key	How it is changed	Effect
Jwt__SigningKey	Write a new value, restart the API	Open sessions end, everyone signs in again. No data is lost
Security__ServerPasswordKey	First plan to enter all server passwords again	Passwords encrypted with the old key cannot be decrypted
Evidence signing key	A new pair is added with a new ID (Keys:2; with the certificate store, a new certificate and CertificateThumbprint), Evidence:Signing:ActiveKeyId = 2 is set	The old public key is never deleted; past evidence files are verified with it. The old private key (or the private key of the old certificate) is deleted
Workers__ApiKey and WorkerApi__Key	The same new value is written on both sides and both are restarted	If the values differ, the Worker does not run
A compromised evidence signing key	First a new key is added and made active (row above), then the moment the old key is believed to have been compromised is written to its Evidence:Signing:Keys:N:RevokedAt field	Signatures made with the old key after that moment count as invalid; earlier ones stay valid. If the active key is revoked, the product signs nothing and nothing runs on Production. The change is recorded as App.ConfigurationChanged

12.5 Trace of settings file changes

Changes in the LDAP, SSO and ITSM sections are detected at API start-up and written to the audit trail as Ldap.ConfigurationChanged, Sso.ConfigurationChanged and Itsm.ConfigurationChanged events.

The same rule applies to the rest of the settings file (session lifetimes, account lockout, password rules, the evidence ledger, MFA, evidence signing, SIEM endpoints and the others): at every start-up the API takes a digest of the effective settings, compares it with the last record and, if there is a difference, writes an App.ConfigurationChanged event with the old and new values and the list of changed keys. A setting overridden by an environment variable appears with its effective value. Secret values are never written, only whether they are set. The first start-up after installation writes the initial state.

If a change relaxes a control, an App.ControlRelaxed event is written as well and goes to the SOC as an alert. These count as relaxing: Auth:MaxSessionHours, Auth:AccountLockoutMaxAttempts and Auth:Password:ExpiryDays increased or set to 0 (no limit); Auth:AccountLockoutMinutes, Auth:Password:MinLength and Auth:Password:HistoryCount decreased; Auth:MfaTicketMaxAttempts, Jwt:AccessTokenMinutes, Jwt:RefreshTokenHours and RateLimiting:PermitPerMinute increased; Auth:Password:RequireUppercase, Auth:Password:RequireDigit, Database:EvidenceLedger, Mfa:Enabled, Mfa:EnforceEnrollment and Evidence:Signing:Enabled switched off; Evidence:Signing:AllowUnsignedProductionExecution and Sandbox:AllowOnProduction switched on;

Evidence:Timestamp:Mode moved away from On; Evidence:Ledger:DigestOutputPath cleared; Evidence:Ledger:DigestIntervalMinutes and Evidence:Ledger:BoundaryCheckMinutes increased. All of these events appear in the Configuration Changes report with record type Configuration. Parameter and mapping changes in the product are always written to the audit trail and go through the four-eyes rule when settings approval is on.

12.7 Ledger digest and evidence write boundary

Once an hour (Evidence:Ledger:DigestIntervalMinutes) the Worker starts a digest round and the API takes a ledger digest from the database. The digest is a single value that covers every ledger record up to that moment. The API signs the digest, writes it to the Evidence:Ledger:DigestOutputPath folder (ledger-digest-...json and, when signing is on, a .sig with the same name; if signing is on but the key cannot be used, no digest file is written and a Ledger.DigestFailed event is written) and adds the Ledger.DigestPublished event to the audit trail. If SIEM is on, the event also goes to the SOC.

These files are the external witness: even if someone who manages the database changes records later, a digest already written to the immutable store does not change. This is why the folder must be in a place that the DBAs and the application server administrators cannot delete or change (WORM share, object lock storage or archive system). The API only writes new files and never overwrites an existing one.

If no folder is defined, the digest still goes to the audit trail and SIEM, but no record is shown as "covered by an external digest".

Monitoring:

- The "Last ledger digest" row on the Governance Readiness screen warns if no digest arrives for two intervals. The same rule is set up in the SOC: an incident is opened if Ledger.DigestPublished does not arrive for two intervals.
- If a digest cannot be produced or written to the folder, the Ledger.DigestFailed event is written.
- In every digest round the latest digest file in the folder is read and compared with the ledger chain of the database. If the database is behind that digest (return to an older backup) or the chain does not match (restore on another server, a change at file level), the Ledger.ForkDetected event is written and a critical notification email is sent. If a restore was planned, its record is matched with this event. When the database is restored, Ledger.RestoreDetected is also written from the msdb restore history.
- If the boundary check fails (section 3.5), the Evidence.BoundaryBroken event is written, a notification email is sent and change operations stop.

Period package. Once a month the package of the month is taken with the Period Package button on the Audit Trail screen and delivered to internal audit. The package is signed when signing is on; it contains every request of the period reconciled row by row between the request table and the audit trail, the ledger digests and the gaps between them, boundary events, restores, Worker outages, the export log

and the approval chain state of each request. A package covers at most 92 days. Its receipt is recorded in the document system of the organisation.

Independent verification. Once a month, not in production but on a copy where a database backup is restored, the auditor or internal audit verifies the ledger with the digests from the immutable store (sys.sp_verify_database_ledger). The steps are in the Auditor Kit document.

12.8 Common problems

Symptom	Possible cause	Fix
API does not start, connection error in the log	ConnectionStrings__Default is wrong or the account lacks permission	Check the connection string and the permissions
API does not start, missing or changed script	AutoMigrate = false and the scripts were not applied or SchemaVersions is incomplete	Section 3.2
API does not start, "The evidence store is not usable"	The database is older than SQL Server 2022 or the evidence table is not a ledger	Install the application database on SQL Server 2022 or later
Saving and approving requests fails with "evidence write boundary is broken"	A trigger was added to the evidence table, the write procedure was changed or an object was added to the evidence schema	The "Evidence write boundary" row on Governance Readiness shows the finding code; the change is undone and the boundary recovers at the next check
No evidence dossier is produced, error "could not be signed"	Signing is on but the key cannot be read (certificate not found, no private key read permission)	Check the certificate and the permission, restart the API
The Oracle execution log shows the warning "the Oracle transaction check could not run"	The target account cannot execute the DBMS_TRANSACTION package (the PUBLIC grant was removed)	GRANT EXECUTE ON SYS.DBMS_TRANSACTION is given to the target account. Until then executions continue, but whether data changes became permanent before an error is not tracked
The ledger digest folder is empty	DigestOutputPath is not defined, the API account cannot write or the Worker cannot reach the API	Check the Ledger lines in the API and Worker logs
Screens open in the browser but no data arrives	The web address is not in AllowedOrigins	Add the web address, restart the API
404 when a page is refreshed	URL Rewrite module is missing	Install the module
Worker does not start	WorkerApi:BaseUrl is wrong or the keys differ	Check the Worker log and both keys
Emails go to one person	Mail:DevMode is true	Set it to false

Symptom	Possible cause	Fix
Directory sign-in reports a configuration error	BaseDn or UserFilter cannot find the person	See the step shown by Test connection
Corporate sign-in gives no role	The mapping value is not the same as the value in the assertion	Use the ReceivedGroups value in the SsoLoginDenied record
An approved ITSM record is not executed	The organisation's state name is not in ItsmReadyStates or the approval field arrives empty	Look at the result of the test on the ITSM screen and adjust the list
No events arrive at the SOC	SiemEnabled is off, the stream is off or there is a connection error	Check the last error and the delivery lag on the SOC / SIEM screen