

SQL Change Guard Installation

Prerequisites Checklist

This document is sent to the IT, database and security teams of the organisation before installation. Its purpose is to remove waiting on installation day: requests for servers, accounts, certificates and firewall rules usually take days inside an organisation. When the items below are ready beforehand, installation day is spent only on installing and configuring the product.

The step by step installation, the meaning of every setting and the details of the integrations are in the Installation and Operations Guide.

1. Overview

SQL Change Guard consists of three parts and runs inside the organisation's network:

Part	What it does	Where it runs
Web interface	The screens users open in the browser	Static site on IIS
API	Runs the business rules, writes to the database, connects to integrations	ASP.NET Core application on IIS
Worker	Runs scheduled and queued work in the background	Windows service

All three can run on the same Windows server. The product's own records are kept in a SQL Server database. Audit records are kept in the append-only ledger table of SQL Server 2022 in the same database.

The product runs inside the organisation and does not need internet access. Exceptions: if it connects to a cloud ITSM (ServiceNow, Jira Cloud), a cloud identity provider (Microsoft Entra ID) or an external timestamp server, outbound HTTPS (443) to that address is needed.

2. Servers

Server	Minimum	Notes
Application server	Windows Server, 4 cores, 8 GB memory, 20 GB disk	The web interface, API and Worker run on this server
Database server	SQL Server 2022 or later, 4 cores, 16 GB memory, SSD	Application database. Audit records are kept in the append-only ledger table that comes with SQL Server 2022. The ledger is available in every edition; Express suits only a pilot or a small organisation (10 GB limit, no encrypted backup). About 10 GB is enough for five years of retention. NTP must be on for the server

The application server and the application database server should be on the same local network.

Software to install on the application server:

Software	Why
IIS (Web Server role)	The web interface and the API are published here
.NET 10 ASP.NET Core Hosting Bundle	To run the API on IIS. The bundle includes the .NET 10 runtime; the Worker uses the same runtime
IIS URL Rewrite module	So that direct links into the web interface open (for example the request link in an email or an ITSM note, and the return from corporate sign-in). A free Microsoft add-on

The API and the Worker can also be installed on separate servers. In that case the Worker receives the product's secrets (the database connection string, encryption keys) from the API at start-up; the evidence signing private key never goes to the Worker; so the connection between the Worker and the API must use HTTPS. If the product detects that this call is made over plain HTTP from a remote address, the Governance Readiness screen shows a warning.

3. Addresses (DNS)

An address is needed for the web interface and one for the API. These addresses are used in several settings and in the web interface package; changing them later requires reconfiguration.

Address	Example	Where it is used
Web interface	https://changeGuard.company.local	The address users open; links in emails and ITSM notes
API	https://changeGuard-api.company.local	Used by the web interface, the Worker and corporate sign-in

The web interface package is prepared with the API address. The API address must therefore be fixed before installation.

4. Certificates

Certificate	For	Required
HTTPS certificate for the web interface and API addresses	Traffic between the browser and the server; corporate sign-in does not work without HTTPS	Yes
Trust for the directory (LDAPS) server certificate	Encrypted connection to the directory. The organisation's root certificate must be in the application server's trust store	If LDAP is used
TLS certificate of the SIEM collector	Encrypted delivery of events to the SOC	If SIEM is used over TLS
SAML signing certificate (.pfx)	If the identity provider requires signed requests	Only in that case

5. Accounts and permissions

5.1 Database accounts

Account	Where	Permission
Application database account	Application database	For the product to install the schema (Database:AutoMigrate = true, the default): db_owner on the database. If the database is not created empty beforehand, the product creates it; the account then also needs database creation permission (dbcreator). If the DBA installs the schema (AutoMigrate = false): the DBA applies the installation scripts, and the application account gets db_datareader, db_datawriter and EXECUTE; the account is also added to the evidence ledger roles (evidence_api_writer, evidence_worker_writer) and gets VIEW LEDGER CONTENT and VIEW DEFINITION on the evidence schema. sysadmin is not needed
Worker database account (optional)	Application database	By default the Worker uses the same account as the API. If a separate account is wanted: db_datareader, db_datawriter, EXECUTE, the evidence_worker_writer role, VIEW LEDGER CONTENT and VIEW DEFINITION on the evidence schema. The API account is then only in the evidence_api_writer role; the database refuses user decisions (approval, rejection, reconciliation decision) and sign-in events written by the Worker account
Target database accounts	Every SQL Server, PostgreSQL and Oracle server to be governed	Permission to perform the operations in approved scripts. In addition the product reads object definitions to generate rollback scripts and object comparisons (VIEW DEFINITION on SQL Server). The Oracle account must also be able to execute the DBMS_TRANSACTION package (on Oracle it is granted to PUBLIC by default; if the organisation has removed that grant, GRANT EXECUTE

Account	Where	Permission
		ON SYS.DBMS_TRANSACTION is given to the account). The product uses this package to read the transaction id before and after every block. These accounts are entered on the product's Servers screen; their passwords are stored encrypted

The connection string is a standard SQL Server connection string. A SQL Server login is recommended. If Windows authentication is used, the database permission must be granted both to the API's IIS application pool identity and to the Worker service account.

5.2 Windows accounts

Account	Permission
Worker service account	Write to the logs subfolder of the Worker folder. Write to the query result file folder (QueryResult:OutputPath, for example D:\SQLChangeGuard\QrFiles).
API application pool identity (IIS)	Write to the logs subfolder of the API folder. Read the query result file folder (for downloads). Create new files in and read the ledger digest folder (6.7). Read the private key of the evidence signing certificate

5.3 Integration accounts (for the integrations in use)

Integration	Account requested from the organisation	Permission
Corporate directory (LDAP / Active Directory)	A read-only service account (full name and password)	Read users and groups. No write permission is needed
Corporate sign-in (SSO)	An application registration (OIDC) or a relying party trust (SAML) at the identity provider	See 6.2
ITSM (ServiceNow, Jira, or others such as ServiceCore through the generic REST connector)	An integration account	ServiceNow: read 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
Email (SMTP)	A sender account	Send email

6. Information to collect from the organisation

Leave the section of an unused integration empty.

6.1 Corporate directory (LDAP / Active Directory)

Information	Example
Directory server name	dc01.company.local
Connection type and port	LDAPS 636 (recommended) or StartTLS 389
Search base for users (BaseDn)	OU=Staff,DC=company,DC=local
Domain name (NetBIOS) or UPN suffix	COMPANY or company.local
Full name of the read-only service account	CN=changepassword-reader,OU=Service,DC=company,DC=local
Directory lockout threshold for wrong passwords	For example 10 attempts. The product's own threshold is kept lower
Directory groups to map to product roles	A list of groups such as CN=DBA-Team,OU=Groups,DC=company,DC=local and the role each one gets

6.2 Corporate sign-in (SSO)

Information	OIDC (Entra ID, Keycloak, Okta)	SAML (AD FS, Entra ID)
Identity provider address	Authority, for example https://login.microsoftonline.com/tenant-id/v2.0	Metadata address, for example https://adfs.company.local/FederationMetadata/2007-06/FederationMetadata.xml
Application registration	Client ID and client secret	Relying party trust
Return address to enter at the identity provider	https://API-ADDRESS/api/auth/sso/callback/PROVIDER-NAME	https://API-ADDRESS/api/auth/sso/saml/acs/PROVIDER-NAME
Group or application role information for role mapping	Application roles in Entra ID (recommended) or group IDs	Role claim
MFA claim	Which claim the identity provider sends when MFA was done (Entra ID: amr = mfa)	AuthnContextClassRef (AD FS: http://schemas.microsoft.com/claims/multipleauthn)

PROVIDER-NAME is the permanent name given to the identity provider during installation (for example Entra). It is not changed after installation.

6.3 ITSM

Information	Example
ITSM product	ServiceNow, Jira Cloud, Jira Data Center, ServiceCore or other
Address	https://company.service-now.com
Integration account and credential type	User name and password; email and API token on Jira Cloud; personal access token on Jira Data Center
Change record state names	In which states the work is implementable (ServiceNow default: Scheduled, Implement); which states are closed
Number formats	Change record (CHG0012345), service request (RITM0012345), incident (INC0012345)
Record types in Jira	Type names used for changes, incidents and service requests
Planned time fields in Jira	IDs of the planned start and end custom fields (for example customfield_10050)
ServiceCore and others	The API address that reads a record, the names of the state, title and approval fields in the response, the address for adding a note

6.4 SIEM / SOC

Information	Example
Collector address and port	siem.company.local, 6514
Protocol	TLS (recommended), TCP or UDP
Format	Rfc5424Json (default), Cef (ArcSight), Leef (QRadar), Json
Thumbprint, if the collector uses a self-signed certificate	

6.5 Email (SMTP)

Information	Example
SMTP server and port	smtp.company.local, 587
Encrypted connection	Yes or no
Sender account, address and display name	changeguard@company.com, SQL Change Guard

6.6 Timestamp (optional)

Information	Example
The organisation's RFC 3161 timestamp server	https://tsa.company.local/tsr
Outbound proxy server (if any)	http://proxy.company.local:8080

6.7 Immutable store for ledger digests

By default, once an hour the ledger digest of the database is written to this folder as a file (signed when signing is on) (Evidence:Ledger:DigestOutputPath). The Worker starts the round; the API takes the digest, signs it (when signing is on) and writes it. When the folder is on a locked store as described below, these files are an external witness that the people who manage the database cannot change afterwards; the lock is provided by the organisation, not by the product. If the path is left empty, no external file is written and the ledger can be verified only against its own internal digest.

Information	Example
Folder path (as seen from the API server)	\\worm.company.local\changeguard-digest
Store type	WORM share, object lock storage or the archive system of the organisation
Lock and retention	Files cannot be deleted or changed; retention is longer than the database backups
Who manages it	A team other than the DBA and the application server administrator

On this folder the API application pool identity only needs permission to create new files and read (reading is used to check continuity with the last digest). The Worker account needs no permission on this folder.

7. Keys generated during installation

The values below are generated inside the organisation during installation and written to the server as environment variables. They are not obtained from outside and are not sent to the SQL Change Guard team. How to generate them is in the Installation and Operations Guide.

Value	Purpose	If lost
Session signing key	Signature of user session tokens	Open sessions end, everyone signs in again
Server password encryption key	Encrypts the database passwords on the Servers screen	Stored server passwords are entered again
Query result package key	Encrypts the passwords of query result files	Passwords of old result files cannot be displayed
Worker key	The Worker identifies itself to the API	The Worker does not run; a new key is written on both sides
Evidence signing key pair	Signs evidence dossiers, audit records packages, ledger digests and period packages. Keeping the private key as non-exportable in the Windows certificate store, not in an environment variable, is recommended	While signing is on and no key is available, no evidence output is produced. The public key and its fingerprint are given to auditors and kept
Installation ID	Shows which installation an evidence file came from (for example COMPANY-PROD-01)	Not a secret; never changed later

Evidence signing is off in the product's code default (Evidence:Signing:Enabled = false). While signing is off, evidence outputs are produced unsigned and requests are not executed on servers defined as Production. For this reason signing is turned on in a production installation and the key pair is prepared before installation.

8. Firewall (port) list

Source	Destination	Port	Purpose	When
User browser	Web interface address	443	Screens	Always
User browser	API address	443	The web interface calls the API from the browser	Always
Worker	API address	443	The Worker receives its configuration and some decisions from the API	Always (local if on the same server)
API and Worker	Application database	1433	Application records	Always
API and Worker	Target databases	1433 (SQL Server), 5432 (PostgreSQL), 1521 (Oracle)	Script execution, connection test, reading object definitions	Always
API and Worker	SMTP server	587 or the organisation's port	Notification emails	If email is on
API	Corporate directory	636 (LDAPS) or 389 (StartTLS)	Authentication and directory synchronisation	If LDAP is used
API	Identity provider	443	Metadata and tokens	If SSO is used
User browser	Identity provider	443	The organisation's sign-in page	If SSO is used
API	ITSM	443	Record lookup and writing notes	If ITSM is used
API and Worker	SIEM collector	6514 or the organisation's port	Delivery of events to the SOC	If SIEM is on
API and Worker	Timestamp server	443 or 80	RFC 3161 timestamps on evidence files	If timestamping is on
API	Ledger digest store	445 (SMB) or the port of the store	Writing the signed ledger digest files	Always (6.7)

No inbound connection to the product is needed from ITSM, the identity provider or the SIEM. The identity provider's return comes through the user's browser.

9. Who does what

Task	Responsible
Servers, IIS, Hosting Bundle and URL Rewrite installation	Organisation IT
DNS records and HTTPS certificates	Organisation IT
Application database, accounts and permissions	Organisation DBA
Firewall rules	Organisation security team
Directory service account, SSO application registration, ITSM integration account	The relevant organisation teams
Preparing the web interface package with the organisation's API address, licence file	SQL Change Guard
Immutable store for ledger digests (6.7)	Organisation storage or archive team
Receiving and recording the period packages	Organisation internal audit
Installation, configuration and post-installation check	Organisation IT together with SQL Change Guard

For the evidence to stay independent, at least these three roles must be held by different people: the DBA, the SIEM administrator and the internal audit that receives the period package. The DBA must not be an operating system administrator on the database server.

10. Installation day checklist

- ☐ Application server ready: IIS, .NET 10 Hosting Bundle, URL Rewrite installed
- ☐ Web interface and API addresses defined in DNS, HTTPS certificates ready
- ☐ Application database on SQL Server 2022 or later, NTP on
- ☐ Application database account and permissions ready (and an empty database created if needed)
- ☐ Immutable store folder for ledger digests ready, the API account can create new files in it and read them
- ☐ Evidence signing certificate in the certificate store of the API server, private key read permission only for the API account
- ☐ Worker service account and query result file folder ready
- ☐ An account ready for at least one target database
- ☐ Firewall rules opened
- ☐ Information for the integrations in use (section 6) collected
- ☐ Installation ID chosen (section 7)
- ☐ SQL Change Guard licence file and web interface package received