SQL Change Guard

User Guide

Screen by Screen Usage

SQL Server | PostgreSQL | Oracle

1. Login and Dashboard

You sign in with your corporate username (LDAP/AD supported; a second factor is requested if MFA is enabled). The dashboard summarizes pending approvals, recent changes, risk distribution and system status.

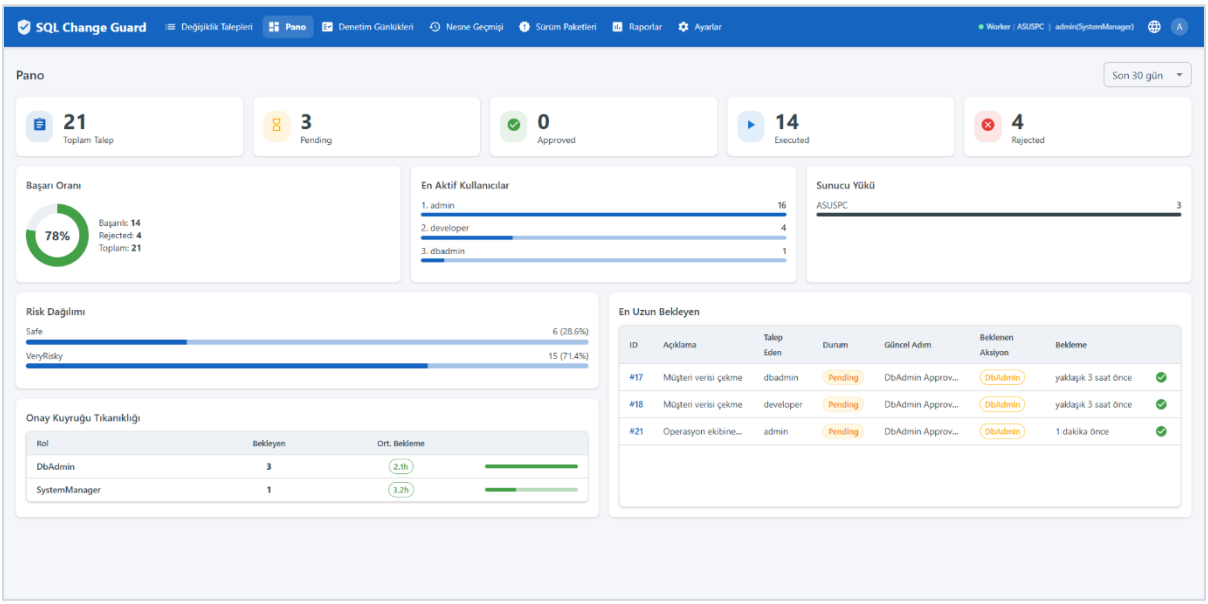
The dashboard keeps two different time meanings apart. The top row counts what happened in the selected date range: requests created, executed, failed executions and rejected. The bottom row counts the current state and does not change with the date selection: pending, waiting execution, running, scheduled within 24 hours and settings awaiting approval.

The execution success rate is successful executions divided by attempted executions. Rejected requests are not part of it; a rejection is a decision, not a failure. When nothing was executed in the range, a dash is shown instead of a rate.

The control exceptions card counts requests that left the normal flow: emergency records, no matching policy, overridden approval step, self approved requests and unmasked data requests without approval. The detail is in the Control Exceptions report and both screens use the same definition.

A request can target more than one server. In the server load breakdown such requests are counted separately for each server; two server names never appear merged in one row.

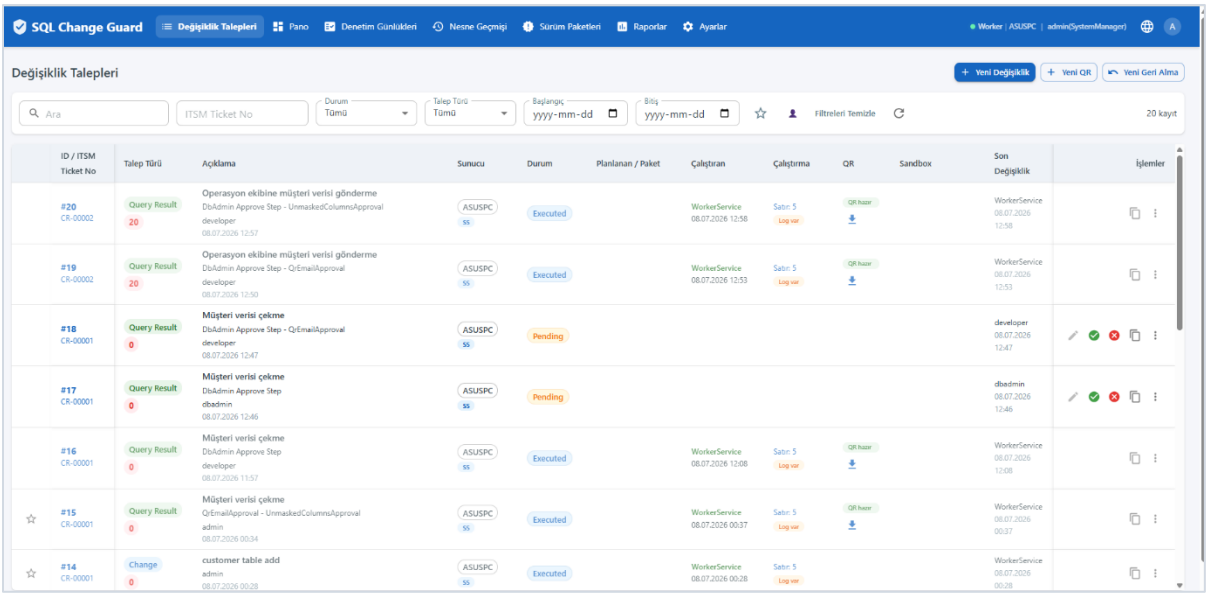
A user without the permission to see all requests sees only their own requests on the dashboard as well. The dashboard never shows what the request list hides.



Dashboard

2. Request List

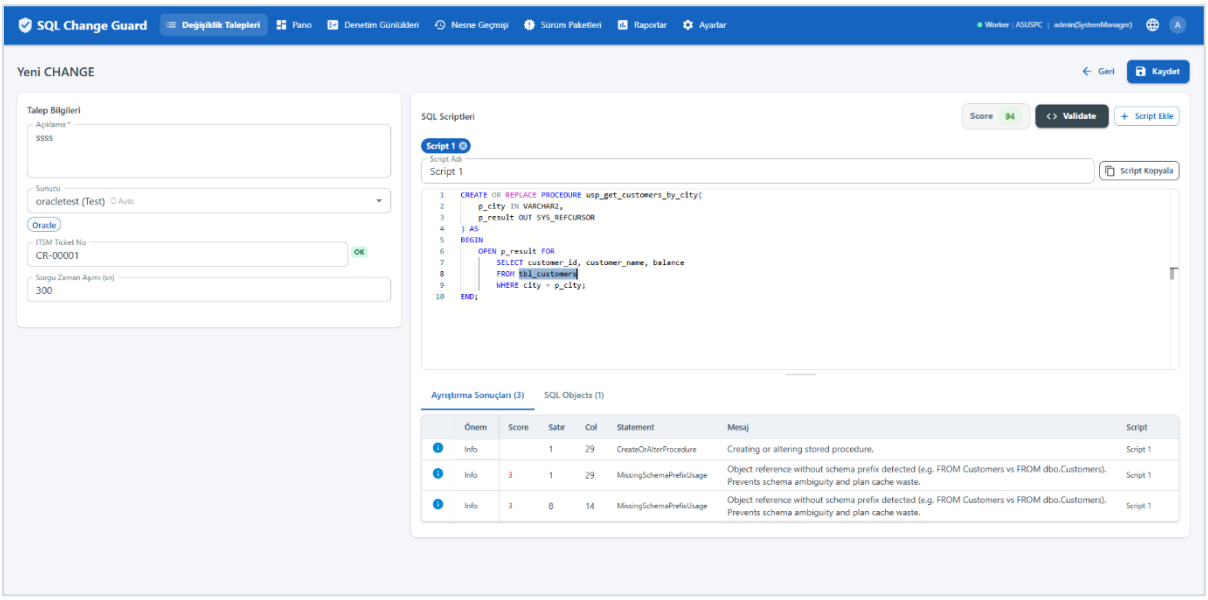
All change and query requests are listed. Filter by status, server, type and text. Each row shows the risk score, status, rollback and release package info. If authorized, approve, execute, schedule and reject actions are performed here.



Request List

3. Creating a Change Request

- Select the server and (if required) the ITSM ticket
- Upload your SQL script; the system parses it automatically and validates with 84+ rules
- The risk score (0-100) and detected warnings are shown instantly
- Click an object in the parse results to jump to the related script block
- On save, the policy engine determines the approval steps



Change Request - automatic parse and risk score

4. Sandbox Validation

Before going live, a change can be validated by running and rolling it back (BEGIN-ROLLBACK) on a real environment. Results are recorded on the request. For Oracle changes containing implicit-commit statements, sandbox runs only for safe (DML-only) scenarios.

5. Approval Workflow

Approval steps are determined by the policy engine per server, environment and type. An authorized role (e.g. DB Admin, Change Manager) approves the step. Under separation of duties, if enabled, a requester cannot approve their own request.

- Segregation of duties settings are defined on the approval policy. There are three: may the requester approve their own request, may the approver execute the same request, does each approval step require a different person. A setting left empty uses the organisation default.
- Only approved requests can be added to a release package. When the package runs, the approval status and the segregation of duties rules are validated again for every request; a package replaces individual execution and never bypasses the approval flow.
- Raising an emergency request is an authority. The minimum role required is set in the Segregation of Duties group on the Parameters screen; users without it do not see the emergency option at all.
- Marking a request as manually applied closes the approval flow, so it follows the same rule as approving and executing: if the requester cannot approve their own request, this path is closed as well.
- Because policies are scoped by server and environment, production can be strict while the test environment stays relaxed in the same system.
- These settings are frozen onto the request when it enters the approval flow. Even if the policy is changed later, the request is evaluated under the rule set it entered with and the evidence dossier shows the rule of that day.
- When each approval step requires a different person, a user closes only one step per action and the remaining steps wait for another approver.
- Once script analysis completes, the request screen shows an "Approval Policy To Be Applied" card. It shows which policy matched, the scope of the match, and for each step whether it is required or will be skipped, including the reason when skipped.
- If the policy produces no approval step for the request, a warning appears when saving. It states clearly that the request will be approved automatically as soon as it is saved and asks for your confirmation.
- The request detail shows the applied policy. Skipped steps are listed with their reasons even for automatically approved requests, and it is stated explicitly when no policy matched.

6. Execution and Rollback

- An approved request can be executed immediately or scheduled
- A rollback script can be generated for each change; a rollback is mandatory for Oracle implicit-commit changes
- Execution runs under a single transaction; rolled back on failure (SS/PG)
- If the source request is edited, the existing rollback is refreshed

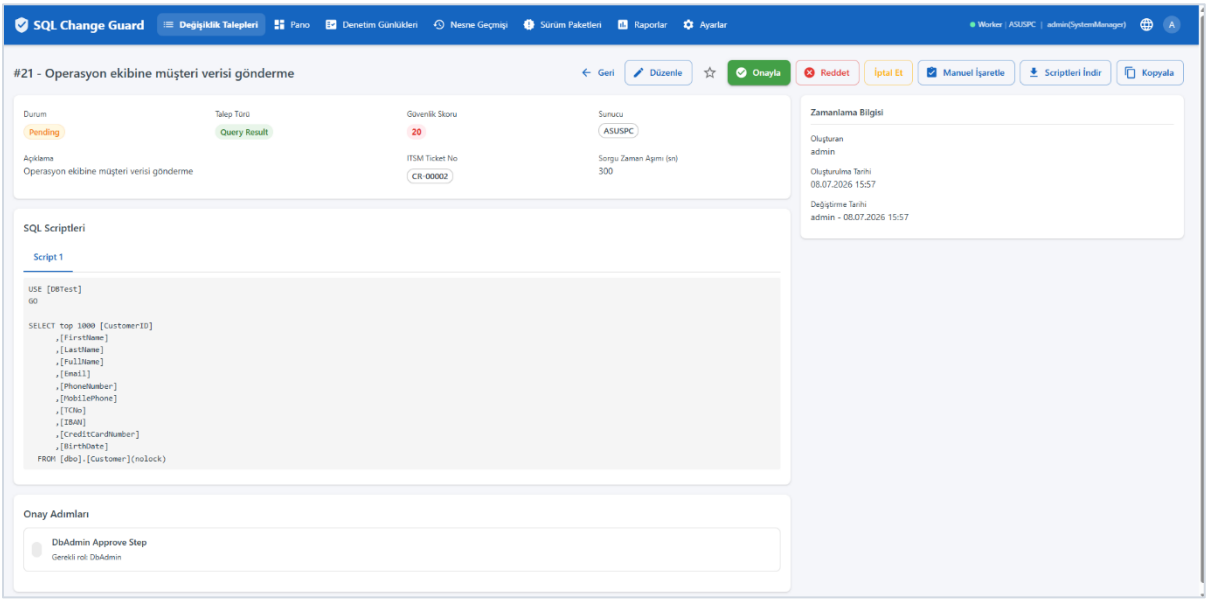
- Execution is carried out by the service, so the request list and detail show WorkerService in the Executor field. The person who pressed the button is recorded separately in the "Started by" field. For an automatic schedule the value is stored as SYSTEM and shown as "automatic schedule". Cancelling the schedule clears the field; the change remains in the audit record as old and new value.

7. Release Packages

Multiple changes are grouped into a single package and executed in dependency order. StopOnError and AllOrNothing modes are supported.

8. Query Result (Production Query)

- Create a SELECT request to one or more servers
- If it touches a critical table/sensitive column, the policy engine applies approval and masking
- Sensitive columns are masked automatically; extra approval is required for unmasked data
- The result is delivered as an encrypted ZIP; a download reason is entered and a download record is kept



Query Result with automatic masking

Delivery mode. The channel used for the result file and for the zip password that opens it is set by an organisation setting. There are three options: portal only (the mail carries neither the file nor the password), zip attached with the password in the portal (the default) and zip and password in the same mail. With the default option the mail carries the file but not the password; the password is only obtained from the request page in the portal.

The organisation setting is a ceiling. The person creating a request may pick a stricter mode but never a looser one; a looser mode is not listed and is rejected on the server even if it is submitted. When zip and password in the same mail is chosen, a written reason is required and that reason appears in the evidence dossier.

To see the password, use the Show zip password button on the request page. The button asks for a reason, then shows the password and lets you copy it. There is no need to download the file again. Who viewed the password, when, and with what reason is written to the audit trail.

When the recipient has no portal account, the person who created the request obtains the password from the portal and passes it on through their own channel. This way the person who accesses the password is always a named user.

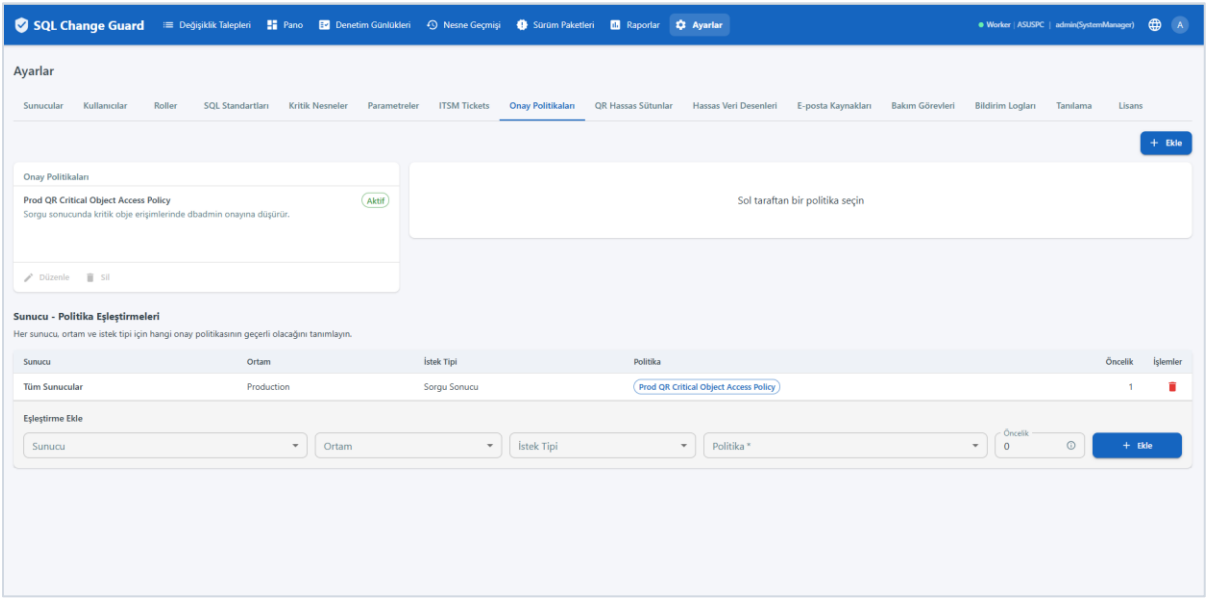
9. Approval Policies and Sensitive Data Patterns

Administrators manage approval policies (server/environment/type), sensitive data patterns (regex) and the critical object list. SQL standard rules are enabled/disabled from the UI and filtered by database type.

In a critical object definition only the object name and the object type are required. The database and schema fields can be left empty: an empty database matches all databases and an empty schema matches all schemas. These fields are shown with an asterisk in the list.

The matching rule is the same for SQL Server, PostgreSQL and Oracle. The object name and the object type must always match, and a database or schema filled in the definition must match as well. An object written without a schema resolves to dbo on SQL Server and to public on PostgreSQL. On Oracle the Package type is used for package units.

- An approval policy cannot be mapped to a server or environment unless it contains at least one approval step. A policy without steps produces no approvals.
- An emergency policy must contain at least one non-skippable approval step, so a request cannot pass through the emergency path without approval.
- The emergency flag of a policy is set only when the policy is created and cannot be changed afterwards. Create a new policy if a different setup is needed.
- These rules are enforced on policy update, step creation, step deletion and mapping. The last step of a mapped policy cannot be deleted.
- The emergency option on the request screen appears only when a suitable emergency policy is defined for all selected servers.

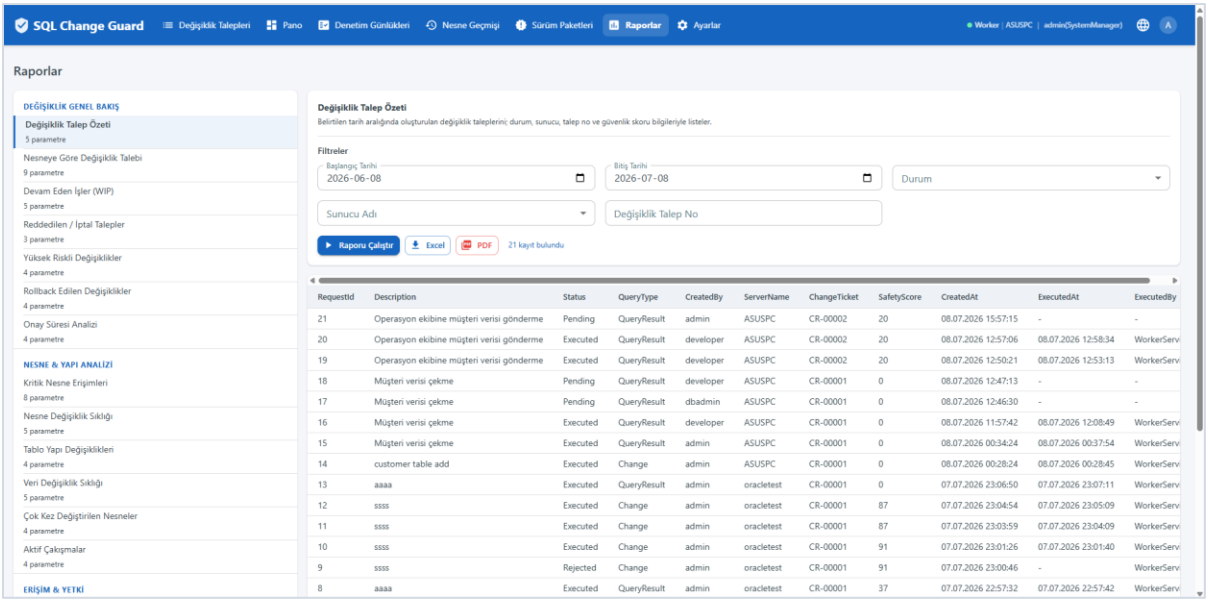


Approval Policies

10. Audit, Reports and Object History

- Audit Logs: full record of DML/DDL/DCL operations
- Reports: 30 built-in reports in five groups, exported to Excel and PDF

- Object History: who, when, which request and which script changed any object
  - Servers: management and settings of multiple SS/PG/Oracle servers



Reports - 30 built-in reports in five groups: Change Governance, Object & Structure, Access & Authorization, Data & Privacy, Configuration & Compliance. Report names and column headers are in English; dates are shown in the local time of the person reading them, on screen and in exports. Reports that carry access, configuration or personal data access evidence are limited to the Auditor, DbAdmin, ChangeManager and SystemManager roles.

The Masking Activity report shows the delivery alongside the masking result. The Delivery Mode column gives the mode that applied to that delivery, the Password In Mail column shows whether the password travelled in the same mail as the file, and the Delivery Reason column carries the written reason entered for that choice. The report shows the mode actually applied at delivery time, not the earlier choice on the request; when the organisation setting was tightened afterwards, the stricter mode applies.

11. Contact

- Web: www.sqlchangeguard.com
- Email: onur.egilmez@sqlchangeguard.com | info@sqlchangeguard.com
- Phone: +90 505 621 29 02
- LinkedIn: linkedin.com/company/sqlchangeguard

New Screen Behaviours

This section summarises what changed on the screens in the latest release.

Users screen. The role list now includes the Auditor role. An auditor only observes, produces evidence and verifies it; they cannot raise, approve or execute a request.

Parameters screen. Parameters that govern how strict a control is now carry a Control setting badge. In the edit dialog, if four eyes approval will hold this change, a warning appears before

saving: the change will not be applied, it will be sent for approval, and the previous value stays in effect until approved.

Request list. Approval steps now appear on a single line under each request: step order, step name, the role that will approve and the person who decided. This answers who will approve without opening the detail screen. Long chains are clipped and the full text appears on hover.

ITSM tickets screen. The ticket number follows the same format rule as the request screen, and a number that breaks the rule is not saved. The title field is mandatory. A ticket number entered on the request screen is added to the list automatically if it is missing, so it becomes selectable for later requests.

Who Did What in Settings Approvals

While the four eyes rule is on, one person requests a settings change and another person holding the same permission approves it. Both names must be visible on the record; otherwise an audit gets a single answer to "who changed this setting" and that answer is incomplete.

The last change column. Every settings screen inside the four eyes scope now carries a new column. The top line shows who changed the record and when. The green badge below shows the approver. When the badge is present the top line carries a Changed by label; without it a single name is shown. Hovering the cell shows the creator, the person who changed the record and the approver on three lines.

Whose name goes on the record. When approval is given the change is applied and the name written on the record is the person who REQUESTED it. The approver is recorded on the settings approval entry and in the audit trail. A single row therefore shows both the requester and the approver.

Two separate audit entries are written. One is the change itself and carries the requester name. The other is the approval entry and carries the approver name, time and IP address. The IP address at approval time belongs to the approver, so it is not written next to the requester; one row carrying wrong information is enough to weaken an audit trail.

The refresh button. Because another user gives the approval, the list on screen can become stale at any moment. The refresh button at the top right of the settings page refreshes the data of the open tab. When a decision is made on the approvals screen, the related screens refresh by themselves.

The settings approvals tab. This tab is visible only to users holding a permission of a screen inside the four eyes scope. Users with view only permissions do not see the tab, because the filtered list would be empty for them anyway.

How Times Are Shown

Every time value in the system is stored in universal time (UTC). Local time is not a property of the data but a presentation choice. Two users in different cities therefore look at the same event and see the same instant; only the text on screen follows their own clock.

On screen. Dates and times are shown in the time zone of your browser. No separate setting is needed.

In documents. PDF, Excel and e-mail are produced on the server, where there is no browser, so the display time zone is read from the installation setting and written onto the document. A reader never has to guess what the time refers to. This choice is deliberate: if the time zone depended on the browser of the person requesting the document, the evidence dossier for the same request would produce two different documents for two auditors.

In date filters. When you pick a date range, the day is your local day. The start day is included from 00.00 and the end day is included until the end of that day.

In the audit trail. Audit records are shown with seconds, so the order of two events inside the same minute can be read.