Setup guide

Install dbriq, connect your servers and set up alerts. About 15 minutes from download to your first findings.

dbriq monitors SQL Server, Azure SQL, PostgreSQL and MySQL from your own Windows PC or server, and tells you in plain words what is wrong and how to fix it. This guide takes you from download to your first findings in about 15 minutes. When you are done, the User guide explains every page of the app.

What you need

Item	Requirement
Computer	Windows 10 or 11, 64-bit. No administrator rights needed.
Browser	Any current browser (Edge, Chrome, Firefox). The dashboard opens at http://localhost:8050.
SQL Server driver	Microsoft ODBC Driver 18 for SQL Server, for SQL Server, Azure SQL and Managed Instance only. PostgreSQL and MySQL drivers are built in.
Network	The PC must reach each database on its port (usually 1433 SQL Server, 5432 PostgreSQL, 3306 MySQL).
Database access	A read-only monitoring login on each server, created with the scripts in step 2.

Supported databases

Engine	Where it runs
SQL Server	2016 SP2 and later on-premises or in VMs; Azure SQL Managed Instance; Amazon RDS for SQL Server; Google Cloud SQL
Azure SQL Database	Single databases and elastic pools
PostgreSQL 10+	Self-hosted; Azure Database for PostgreSQL; Amazon RDS and Aurora; Cloud SQL
MySQL and MariaDB	MySQL 5.7 and 8.x; MariaDB; Azure Database for MySQL; Amazon RDS and Aurora; Cloud SQL

Beta: start with a non-production server, then add production once you are comfortable with what it does.

Step 1: Install dbriq

Installing takes about two minutes and needs no administrator rights. dbriq installs into your own user folder and opens with demo data, so you can look around before connecting a real server.

1. Sign in at dbriq.com and download the installer from the download page.
2. Before opening the download, right-click it, choose **Properties**, tick **Unblock** at the bottom of the General tab, and click **OK**. This stops the blue Windows warning, because dbriq is not yet code-signed.
3. If you downloaded a ZIP, right-click it, choose **Extract All**, and open the extracted folder.
4. Run the installer. If Windows still shows "Windows protected your PC", click **More info**, then **Run anyway**.
5. Choose whether to add a desktop icon and whether to start dbriq when you sign in to Windows, then click **Install**.
6. If Microsoft ODBC Driver 17 or 18 for SQL Server is missing, the installer offers to open Microsoft's download page. Install the 64-bit driver if you will monitor SQL Server, Azure SQL or Managed Instance. You can skip it for PostgreSQL and MySQL.

7. Leave **Open dbriq** ticked and click **Finish**.

dbriq opens in your browser at http://localhost:8050 and adds a dbriq icon to the Windows notification area (system tray). Right-click that icon for **Open dashboard** or **Quit dbriq**.

> **Company laptop?** A message such as "Your organization has blocked this app" means your IT team must approve dbriq first. Send them the download link and the SHA-256 checksum shown on the download page.

The demo estate

Until you add your first server, dbriq shows a built-in demo: seven servers and about 100 databases with realistic problems such as blocking, a slow query and a log filling up. A **Demo data** label sits at the right end of the top menu. Use it to learn the pages in the User guide. The demo switches off automatically when you add a real server.

Step 2: Create the monitoring login

dbriq connects to each server with its own read-only login, named `dbriq` in the scripts. Run the matching script once per server as an administrator. The scripts are in the Start menu under **dbriq > Setup scripts**.

In every script, replace `<use a strong password>` with a real password and keep it for step 3. None of the scripts give dbriq permission to change data or settings.

Engine	Script	What it grants
SQL Server (on-premises, VM) and Managed Instance	`setup_monitoring_user.sql`, SQL Server section	VIEW SERVER STATE and VIEW ANY DEFINITION; a user in each monitored database; SELECT on the specific msdb backup and Agent job tables
Azure SQL Database	`setup_monitoring_user.sql`, Azure SQL Database section	A login in master; VIEW DATABASE STATE and VIEW DEFINITION in each database

Engine	Script	What it grants
Amazon RDS for SQL Server	`setup_monitoring_user.sql`, RDS section	Run as the RDS master user; same permissions as SQL Server
PostgreSQL	`setup_monitoring_postgres.sql`	The built-in `pg_monitor` role, plus CONNECT on each database
MySQL and MariaDB	`setup_monitoring_mysql.sql`	PROCESS, SELECT on `performance_schema` and `sys`, REPLICATION CLIENT

Set up dbriq with an earlier version? Your existing `sqlmonitor` login and its `sqlmonitor_*` event sessions keep working, so there is no need to recreate them.

Engine-specific notes

- **SQL Server:** on SQL Server 2022 and Managed Instance, the script shows newer, narrower permissions you can use instead. dbriq deliberately does not read Agent job step commands or Database Mail content, which often contain secrets.
- **Azure SQL Database:** run part 3 of the script in each database as an admin. It creates a small in-memory deadlock capture, because Azure SQL Database keeps no deadlock history a monitoring login can read.
- **PostgreSQL:** query statistics need the `pg_stat_statements` extension. Add it to `shared_preload_libraries`, restart PostgreSQL, then run `CREATE EXTENSION pg_stat_statements;`. Without it, everything except top queries still works.
- **MySQL:** `performance_schema` must be on. It is on by default in 5.7 and later; on Amazon RDS, check the parameter group.

Optional extras

- **Client timeouts report:** the always-on `dbriq_attention` event session in the script. Without it, the report offers a one-minute capture, which needs ALTER ANY EVENT SESSION.
- **Parameter sniffing histograms:** `GRANT SELECT ON SCHEMA::dbo TO dbriq;` in the databases where you want histogram evidence.

Without the msdb permissions, backup, job and CHECKDB checks are skipped and everything else still works.

Step 3: Add your servers

Adding a server takes about a minute, and dbriq shows its first figures within 15 seconds. Adding the first real server switches off the demo data.

1. Click **Servers** in the left menu, then **Add server**.
2. Fill in the form, using the table below.
3. Click **Test connection**. Fix any error it reports (see Troubleshooting), then click **Add server**.
4. Repeat for each server. One installation monitors up to 100 servers.

Field	What to enter
Database engine	SQL Server, Azure SQL, PostgreSQL or MySQL
Display name	A short name shown on the estate, in alerts and in search, such as `prod-sql-01`
Server address	Host name or IP address, such as `sql01.corp.local` or `myserver.database.windows.net`
Port	Filled in for the engine; change it only if your server uses another port
Authentication	SQL login (the `dbriq` login from step 2), Windows authentication, or a Microsoft Entra option for Azure (password, service principal, interactive with MFA, or your Azure CLI sign-in)
User name and password	The monitoring login and its password
ODBC driver	SQL Server family only; choose ODBC Driver 18 if it is listed
Trust server certificate	SQL Server only. Tick only for internal servers with self-signed certificates; leave it off for Azure and AWS
SSL	PostgreSQL and MySQL. Keep **Required (recommended)**

Field	What to enter
Maintenance database	PostgreSQL only. The database where `pg_stat_statements` is installed, usually `postgres`
Databases	**All online databases**, or **Only these databases** with a list
Skip these databases	Optional, comma separated, such as `master, tempdb_copy`

Security: passwords are stored in Windows Credential Manager, never in a settings file.

What happens next

dbriq collects on four schedules, all changeable under **Settings**:

Schedule	Every	What it collects
Fast	15 s	CPU, sessions, blocking, waits, running queries, pool usage
Standard	60 s	Query statistics and plans, deadlocks, IO latency, memory grants
Slow	10 min	Space, missing indexes, statistics, Query Store regressions, configuration
Index scan	12 h	Index fragmentation, at most two databases at a time

Every monitoring query has a 30-second timeout. Health checks and top-query history fill in over the first hour; baselines for anomaly alerts need about a week of history.

To take a server out of monitoring for a while, click **Pause** on the Servers page. **Remove** stops monitoring and deletes its saved password.

Step 4: Set up alerts and settings

dbriq works with its default settings, but most teams spend ten minutes on alert routing and maintenance windows. Everything below is under **Settings** in the left menu; click **Save settings** after changes.

Send alerts to your team

Under **Notification routes**, add one route per destination. Every alert goes to each route it matches.

1. Choose the **Type**: Slack incoming webhook, Microsoft Teams webhook, PagerDuty (Events API v2), or Generic webhook (JSON).
2. Give it a **Name**, and paste the **Webhook URL or routing key**.
3. Under **Servers**, enter `*` for all servers, or names and wildcards such as `prod-*`.
4. Choose the **Minimum severity**: Warning and critical, or Critical only.
5. Click **Add route**, then **Send test** to check it arrives.

A common setup is Slack or Teams for all warnings, and PagerDuty for `prod-*` critical alerts only.

Maintenance windows

Under **Maintenance windows**, add the times when patching, index rebuilds or backups normally cause spikes. dbriq raises no new alerts or notifications during them.

Alert thresholds

Alert thresholds has a master switch, one switch and limit per metric (CPU, IO, log, blocking, space and others), and a separate switch for anomaly alerts. Anomaly alerts compare each value with what is normal for that weekday and hour, so they need about a week of history before they fire.

What to collect

Under **Collection**, each feature has its own switch: wait sampling, query statistics, execution plans, deadlock capture, index scans, change detection, time-travel snapshots, baselines and the advisor. Switching one off stops that work on your servers, not just the display. You can also change the collection schedules here.

Health checks and **Cost analysis** have the same kind of switches, plus an exclusion list per check, such as `sqlvm-erp01/Archive*` or `*/ReportServer*`.

Explain with AI (optional)

Under **AI assistant**, turn on **Explain with AI** and paste an Anthropic API key from console.anthropic.com. Each finding then gets an **Explain with AI** button. dbriq sends the finding and

the query with every literal value masked; turn off **Include query text** if even the query structure is confidential.

Email (optional)

The **Email** section is used only for password-reset codes when sign-in is on (step 5). Enter your SMTP server, port, security, sign-in and From address, then **Send test**. Alerts go through notification routes, not email.

History

dbriq keeps 14 days of history by default, in a small database in its data folder.

Step 5 (optional): Share dbriq with your team

For one DBA, the desktop app is enough. For a team, install dbriq once on a server; everyone then opens an address such as `https://dbriq.corp.example.com` and signs in. The browser talks HTTPS to IIS or Caddy, which passes requests to dbriq on the same server only.

Windows Server with IIS

1. On the server, run the installer and choose **Install for all users**.
2. Install two free IIS modules from Microsoft: **URL Rewrite** and **Application Request Routing**.
3. Get a DNS record (for example `dbriq.corp.example.com`) pointing to the server, and a certificate with that name. Import it into **Local Computer > Personal** and note its thumbprint.
4. In PowerShell as Administrator, in `C:\Program Files\dbriq\deploy\windows`, run:

```
.\Install-DbriqServer.ps1 -HostName dbriq.corp.example.com -CertificateThum
```

It asks for the first admin's password, then sets up the data folder, background service, IIS site and firewall. To try it before you have a certificate, use `-SelfSignedForTesting` instead of `-CertificateThumbprint`; browsers will warn.

Then open the address, sign in as the admin, and add each DBA under **Settings > Users** with a temporary password.

To sign in to SQL Server with Windows authentication, run the service as a group managed service account with `-ServiceAccount 'CORP\gmsa-dbriq$'`. Use `-AppPort` if port 8050 is taken.

Back up `C:\ProgramData\dbriq`, including `keys\vault.key`. Without that key, the saved server passwords cannot be decrypted.

Linux or Docker

`deploy/linux/docker-compose.https.yml` runs dbriq with Caddy in front:

1. Put your certificate in `deploy/linux/certs` and set the host name in `Caddyfile`.
2. Create `sqlmon_key.txt` (the credential vault key) and a `.env` file with the first admin's name and password.
3. Run `docker compose -f docker-compose.https.yml up -d`.

Users and roles

Role	Can do
Viewer	Read everything; change nothing
Operator	Acknowledge alerts, pause servers, add change markers, run captures, use AI explanations
Admin	Everything, including servers, settings and users

Users must choose their own password (12 or more characters) at first sign-in. Closing the browser signs them out, as do 30 idle minutes (changeable under **Settings > Access**), and every sign-in ends after 12 hours. Five wrong passwords lock that user name for 15 minutes. Every sign-in and change is recorded in the audit log under **Settings**.

To use Windows or Entra ID sign-in instead of passwords, put an authenticating proxy in front (IIS Windows authentication, Azure App Service authentication, or oauth2-proxy) and choose **Single sign-on via reverse proxy** under **Settings > Access**.

Updating, data and uninstalling

Updating to a new version

Download the new installer from dbriq.com and run it over the existing installation. Your servers, settings, history and saved passwords are kept. Quit dbriq first from the tray icon, or the installer will close it for you.

Where dbriq keeps its data

Installation	Data folder
Desktop app	`%APPDATA%\dbriq` (settings, history and logs)
Team server on Windows	`C:\ProgramData\dbriq`
Docker	The `/data` volume

Server passwords are kept in Windows Credential Manager on the desktop, or in an encrypted vault on a team server. To move a team server, back up the whole data folder including `keys\vault.key`; without that key the saved passwords cannot be read.

Uninstalling

1. Open Windows **Settings > Apps > Installed apps**, find **dbriq**, and choose **Uninstall**.
2. dbriq asks whether to remove all its data. Choose **Yes** to delete your servers, settings, history, logs and saved passwords. Choose **No** to keep them for a later reinstall.

Uninstalling never changes your database servers. To remove the monitoring login as well, drop the `dbriq` login and users on each server, and any `dbriq_*` event sessions you created.

Troubleshooting

Most problems show up as a clear message under **Test connection**, or in the **Collection errors** panel on the Estate page. Find the message or symptom below.

Connecting to servers

Message or symptom	Fix
Login failed	Check the user name and password, and that the `dbriq` login exists on that server
The login works but has no user in this database	Run `CREATE USER dbriq FROM LOGIN dbriq;` in that database

Message or symptom	Fix
The login can't read performance data	Grant VIEW SERVER STATE (instances) or VIEW DATABASE STATE in each database (Azure SQL Database), as in the setup script
Azure blocked this computer's IP address	In the Azure portal, add the PC's IP address under the server's **Networking** settings, then wait about 5 minutes
The ODBC driver isn't installed ("Data source name not found")	Install Microsoft ODBC Driver 18 for SQL Server (64-bit), or pick an installed driver in the server's settings
Certificate chain not trusted	For an internal server with a self-signed certificate, tick **Trust server certificate**. Leave it off for Azure and AWS
Timeout, or server shows Unreachable	Check the address and port, and that firewalls and VPNs let the PC reach the server

Missing information

Symptom	Cause and fix
No top queries on PostgreSQL	`pg_stat_statements` isn't loaded. Add it to `shared_preload_libraries`, restart, and run `CREATE EXTENSION pg_stat_statements;`
No top queries on MySQL	`performance_schema` is off. Turn it on (on Amazon RDS, in the parameter group) and restart
No backup, job or CHECKDB checks	The login can't read msdb. Run the msdb part of the setup script
No deadlocks on Azure SQL Database	Run the deadlock capture part of the setup script in each database

Symptom	Cause and fix
A page or feature shows nothing at all	It may be switched off under **Settings > Collection**, **Health checks** or **Cost analysis**
No anomaly alerts yet	Baselines need about a week of history

The app itself

Symptom	Fix
Windows shows "Windows protected your PC"	Right-click the download, choose **Properties**, tick **Unblock**, then run it; or click **More info**, then **Run anyway**
"Your organization has blocked this app"	Your IT team must approve dbriq; send them the download link and SHA-256 checksum
The dashboard doesn't open	Right-click the dbriq tray icon and choose **Open dashboard**. If port 8050 is busy, dbriq uses the next free port
Alerts don't reach Slack, Teams or PagerDuty	Click **Send test** on the route; check the webhook URL, the route's servers and minimum severity, and that no maintenance window is active

Logs and help

The log file is `dbriq.log` in the data folder (`%APPDATA%\dbriq` on the desktop). Attach it when you report a problem.

Email support@dbriq.com with what you saw, a screenshot, your dbriq version and the log file. Please report security issues to security@dbriq.com.