



CUSTOMER GUIDE

JSBS Core Database Installer Guide

Installation & Team Connection

Install the shared database, add workspace users, and connect every workstation

Database Installer 1.9.0 | JSBS Core 1.6.0 | Schema 23

Prepared by JS Business & Services, DBA JSBS Co.

[START HERE](#)

About this guide

Use this guide to prepare one Windows computer as the shared JSBS Core Team database host, then connect the first administrator and every authorized user workstation.

CURRENT MATCHED RELEASE This edition describes Database Installer 1.9.0, which creates or upgrades database schema 23 for the JSBS Core 1.6.0 release family. Check the compatibility line in later Core release notes before maintenance.

Who should use it

Server administrator	Downloads and runs the Database Installer with Windows administrator approval, selects the local database location and port, and protects the backup and connection details.
JSBS Core administrator	Connects first, creates workspace user accounts, and assigns module view/write permissions.
Each JSBS Core user	Installs and licenses Core on an approved device, selects Company server, enters the shared connection details, and confirms access.

Screenshot note

The screenshots are rendered from the actual JSBS Core WPF screens with fictional names, a fictional server, and an example-only connection key. Your values will be different.

HOW IT WORKS

One server, one shared workspace

Team users run the same JSBS Core application on their own Windows computers. Each copy talks to one Firebird database service on the designated server computer.

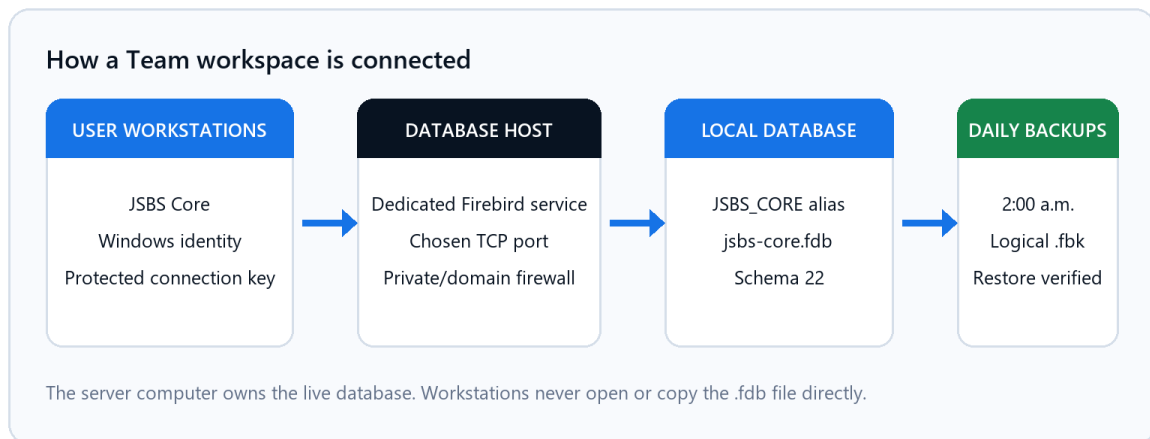


Figure 1. Team connection and backup flow.

- The live .fdb database stays on a local disk in the server computer. Workstations connect over the network and never open the file through a shared folder.
- Every workstation uses the same server name, port, database alias, and connection key. Windows protects the key separately for each signed-in Windows user.
- Workspace identity and permissions come from the user's exact Windows identity; the shared connection key is not a substitute for user authorization.
- A Team or Universal Perpetual v1 license unlocks shared workspace-user administration. License device limits remain separate from the number of database users.

HOW IT WORKS

What the Database Installer changes

The Database Installer is an unlicensed administration utility. It prepares and maintains the shared server; JSBS Core itself still requires a valid license on every applicable user/device.

Dedicated service	Installs a dedicated Firebird 5.0.4 service that starts with Windows and listens on the selected port.
Local database	Creates jsbs-core.fdb in the selected local folder. The default is C:\ProgramData\JSBS Core\Database.
Secure connection	Creates protected database credentials, requires Firebird wire encryption, and uses the fixed database alias JSBS_CORE.
Firewall	Optionally creates one inbound TCP rule for the selected port on Private and Domain network profiles only.
Schema	Creates a new schema 23 database or applies the supported migrations to an older Team database.
First administrator	New setup creates the first administrator from the exact workstation Windows identity. Repair keeps existing users and permissions.
Verification	Tests a workstation-style network connection and confirms that the database is on the expected schema.
Daily backup	Schedules a 2:00 a.m. logical backup in C:\ProgramData\JSBS Core\Backups and restores it to a temporary database to verify recoverability.

DO NOT EDIT SERVER FILES Do not move, rename, copy, or open the live .fdb file directly. Use the Database Installer for Team schema maintenance and a planned, verified recovery process for relocation or restore.

BEFORE INSTALLATION

Prepare the server and account details

1. **Choose the database host.** Use a 64-bit Windows computer that is reliably available whenever the team works. It must have a local disk location for the database.
2. **Sign in as a Windows administrator.** The installer must create protected folders, a Windows service, a firewall rule, and a scheduled task.
3. **Confirm the network profile.** Use a trusted Private or Domain network. The standard firewall option intentionally does not expose the database on a Public profile or the internet.
4. **Choose the first JSBS Core administrator.** Record the exact Windows identity used on that person's Core workstation, such as NORTHSTAR\morgan.lee or DESIGN-PC\morgan.
5. **Choose the port.** Use 3050 unless another service already uses it. If you choose 3051 or another allowed port, every workstation must use the same value.
6. **Download from the approved delivery page.** Use the Team or Universal purchase/download portal and keep the installer on the server computer.
7. **Plan backup protection.** The installer creates a verified daily backup on the server. Also protect copies outside the same computer or failure domain according to your organization policy.

IMPORTANT FOR WORKGROUPS The installer initially suggests the Windows account currently running on the server. If the Core administrator works from a different non-domain computer, replace that suggestion with the administrator workstation's exact COMPUTERNAME\username identity.

INSTALL ON THE SERVER

1. Download and open the installer

Perform these steps on the computer that will host the Team database.

1. **Download the Team Database Installer.** From the verified post-purchase page, download JSBS-Core-Database-Installer.exe.
2. **Confirm the source.** Use only the file downloaded from the JSBS purchase portal. Do not use a copy forwarded by email or found on an unrelated website.
3. **Open the file.** Double-click it. Windows asks for administrator approval because the installer creates a Windows service.
4. **Handle a reputation warning carefully.** If Windows shows a protection warning, confirm the filename and approved download source before choosing More info and Run anyway. Stop if the source is uncertain.
5. **Approve User Account Control.** Choose Yes or enter an administrator credential. The Database Installer window opens.
6. **Check the displayed version.** The update card should show Version 1.9.0 for this guide. Choose Check for updates if you want the installer to look for a newer verified release before setup.

UPDATE DOWNLOADS ARE SEPARATE Installing a verified Database Installer program update does not silently change the server database. After the installer restarts, review Server settings and choose Install database server or Repair or update server.

INSTALL ON THE SERVER

2. Configure Server settings

Review every field before starting. The first administrator identity and port are especially important for a successful workstation connection.



JSBS Core Database Installer

Set up this Windows computer as the shared Team database host

What this installer does

Installs a dedicated Firebird service, creates the JSBS Core database on this computer's local disk, opens only the private/domain firewall port, and configures verified daily backups.

Server settings

DATABASE FOLDER

C:\ProgramData\JSBS Core\Database

Browse

The database stays on a local disk in this server computer. Workstations connect over the network.

NETWORK PORT

3050

FIRST JSBS CORE ADMINISTRATOR

NORTHSTAR\morgan.lee

On the first Core workstation, choose Company server and Copy account. Paste that exact Windows account here, for example COMPANY\engineer. This server's login may be different.

☒ Allow JSBS Core through Windows Firewall on private and company networks

The server's trusted company network must be Private or Domain in Windows. Public networks are not opened by

Administrator approval is required because this installs a Windows service.

Cancel

Install database server

Figure 2. Database Installer Server settings with fictional training values.

Database folder	Use the default or another empty folder on a local disk. Do not choose a network share, mapped drive, drive root, or nonempty unrelated folder.
Network port	Keep 3050 unless it is already used. The installer accepts ports 1024 through 65535.
First administrator	Enter the exact Windows identity that will manage JSBS Core users and permissions.
Firewall option	Leave checked on a trusted Private/Domain network. If IT manages the firewall, request the selected inbound TCP port.

INSTALL ON THE SERVER

3. Run the installation and wait for verification

1. **Select Install database server.** The settings become read-only while the operation runs.
2. **Watch the progress message.** The installer protects folders and credentials, verifies the bundled Firebird package, configures the database engine, and creates or migrates the JSBS Core schema.
3. **Allow service and firewall setup.** The installer starts the dedicated service and applies the selected Private/Domain firewall rule.
4. **Wait for the local server check.** The installer checks TCP and database schema from the server itself. This does not verify another workstation; run the Core connection check on each client next.
5. **Wait for backup scheduling.** The installer places a maintenance copy of itself on the server and schedules the daily restore-verified backup.
6. **Do not close early.** Continue only after the green Server installed · local check passed panel appears.

EXISTING TEAM DATABASE Repair or update server creates and restore-verifies a safety backup. It keeps existing users, permissions and connection credentials, and requires an active administrator. It does not use the server login to replace the first administrator or relocate the database.

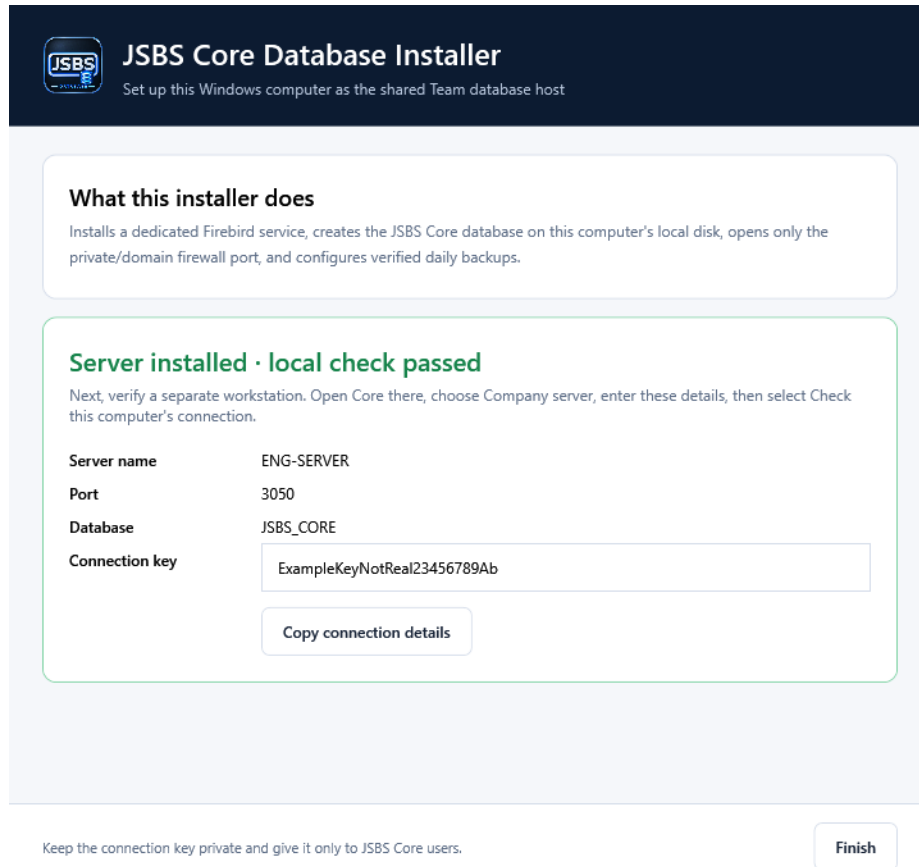
If installation stops

Read the red error message, correct the specific folder, port, administrator, service, or firewall issue, and try again. The installer is designed to stop instead of taking ownership of an unsafe folder or applying an unsupported database change.

INSTALL ON THE SERVER

4. Copy and protect the connection details

The ready panel contains the information every approved Core workstation needs.



The screenshot shows the 'JSBS Core Database Installer' window. The title bar is dark blue with the JSBS logo and the text 'JSBS Core Database Installer'. Below the title bar, it says 'Set up this Windows computer as the shared Team database host'. The main content area has a light blue background. It contains a section titled 'What this installer does' with a description: 'Installs a dedicated Firebird service, creates the JSBS Core database on this computer's local disk, opens only the private/domain firewall port, and configures verified daily backups.' Below this is a green-bordered box titled 'Server installed · local check passed'. Inside this box, it says 'Next, verify a separate workstation. Open Core there, choose Company server, enter these details, then select Check this computer's connection.' Below this text is a table with the following details: Server name: ENG-SERVER, Port: 3050, Database: JSBS_CORE, and Connection key: ExampleKeyNotReal23456789Ab. There is a 'Copy connection details' button below the connection key. At the bottom of the window, there is a 'Finish' button and a note: 'Keep the connection key private and give it only to JSBS Core users.'

Server name	ENG-SERVER
Port	3050
Database	JSBS_CORE
Connection key	ExampleKeyNotReal23456789Ab

Copy connection details

Keep the connection key private and give it only to JSBS Core users.

Finish

Figure 3. Successful server setup with fictional connection details.

1. **Choose Copy connection details.** The server name, port, JSBS_CORE database alias, and connection key are copied together.
2. **Store the details securely.** Use an approved password manager or similarly protected administrative record. Treat the connection key as a password.
3. **Share only with approved users.** Send the details through a secure channel. Do not place the connection key in a public document, ticket, group chat, or unprotected email.
4. **Choose Finish.** Leave the server powered on and connected to the trusted company network.

FICTIONAL KEY The connection key shown in Figure 3 is not real and cannot connect to a database. Your installer generates a different random key.

CONNECT JSBS CORE

5. Connect the first administrator

Use the Windows account entered as First JSBS Core Administrator. Connecting from a different identity does not grant administrator rights.

Set up JSBS Core

How will you use JSBS Core?
Choose a private database on this computer or connect to the shared JSBS Core Server your company installed.

Licensed access: Solo + Team

☐ **This computer only**
Solo
Uses a private embedded database and opens no network port.

☒ **Company server**
Team
Multiple users connect to a database installed by JSBS Core Database Installer.

COMPANY SERVER

Your Windows account
NORTHSTAR\morgan.lee Copy account

Give this exact account to your Team administrator. For a new server, enter it as the first Core administrator in Database Installer.

Server name or IP Port
ENG-SERVER 3050

Server connection key
.....

Enter the key displayed when JSBS Core Database Installer finishes. Windows protects it for this user.

Check this computer's connection

Exit setup Connect to server

Figure 4. Company server selected with fictional training connection values.

1. **Install JSBS Core.** Use the approved installer on the administrator workstation.
2. **Open Core and activate the license.** It must include Team access; Database Installer does not activate Core.
3. **Select Company server.** This computer only creates a separate Solo database.
4. **Enter Server name or IP.** Use the copied server name, or its stable local IP if name resolution is unavailable.
5. **Enter Port and connection key.** Use the exact copied values. The database alias JSBS_CORE and database user are handled automatically.
6. **Check this computer's connection.** Run the check for server name, network port, database key, schema and this Windows user. Resolve the first failing stage. Then choose Connect to server to save the protected profile and open the workspace.
7. **Confirm administrator access.** The upper-left identity should show the expected display name/Windows identity and Administrator role.

CONNECT EVERY USER

6. Add workspace users before they connect

The first administrator should create one active workspace account for each approved Windows identity and assign only the modules that person needs.

Users
Windows identities approved for this workspace
JSBS Team - 2 active workspace user(s). Each user/device requires applicable licensing.

Avery Chen
NORTHSTAR\avery.chen

Morgan Lee
NORTHSTAR\morgan.lee
Administrator

[+ Add Windows user](#)

WINDOWS IDENTITY
NORTHSTAR\avery.chen

DISPLAY NAME
Avery Chen

Active account ☒

Administrator ☐

MODULE	VIEW	WRITE
Dashboard	☒	☐
Work Planning	☐	☐
Projects	☒	☒
CAD Tracker	☒	☒
Project costing	☐	☐
Engineering Change Orders	☒	☐
Manufacturing Notes	☒	☒
Tasks	☒	☒
Bills of Materials	☒	☐
Standards	☒	☐

Editing Avery Chen. Changes apply when this user reopens Core.

[Save user & permissions](#)

Figure 5. Users & permissions with fictional users and mixed view/write access.

1. **Open Settings > Users & permissions.** Only a JSBS Core administrator with Team access can add and manage shared workspace users.
2. **Choose + Add Windows user.** A blank user form opens.
3. **Enter the exact Windows identity.** Use COMPANY\username for a domain account or COMPUTERTNAME\username for a local account. Ask the user to run whoami and send the exact result securely.
4. **Enter a clear display name.** This is the friendly name shown in assignments and user lists.
5. **Keep Active account on.** Turn on Administrator only for a person who must manage shared configuration and users.
6. **Set module permissions.** View permits review; Write allows changes. Projects access does not grant costing access. Grant Project costing View separately for cost review and Write for changes. Existing non-administrators start with no costing access; administrators retain access.
7. **Choose Save user & permissions.** The access takes effect the next time that Windows identity opens JSBS Core.
8. **Repeat for every user.** The shared database key is common, but each person's identity and permissions are individual.

CONNECT EVERY USER

7. Set up each workstation

Repeat this procedure while signed into Windows as the person who will use JSBS Core. The connection profile and protected key belong to that Windows account.

1. **Confirm the account was added.** Ask the Core administrator to verify the exact Windows identity, Active account switch, and module permissions.
2. **Install JSBS Core.** Use the approved Core installer on the user's device.
3. **Activate the assigned Core license.** Use the license provided by the organization. Each user/device must have applicable licensing even though workspace-user count and device activation limits are separate controls.
4. **Select Company server.** Enter the same server name or stable local IP, port, and shared connection key used by the first administrator.
5. **Check this computer's connection.** Verify the name, port, key, schema and current Windows identity. Then choose Connect to server and wait for the shared workspace.
6. **Check identity and role.** Verify the upper-left name and role match the workspace account. Stop if a different identity appears.
7. **Check connection status.** The lower-left status should identify the JSBS Core Server/shared Team database and show a healthy connection.
8. **Test real access.** Open the user's normal modules. Confirm read-only versus write behavior with a safe test appropriate to the workspace.

SHARED COMPUTERS If several people use one workstation under separate Windows sign-ins, each person must launch Core and save the Team connection under their own Windows session. Do not share one Windows account to bypass user identity or licensing controls.

VERIFY THE DEPLOYMENT

8. Confirm the Team workspace is ready

Server service	Restart the server during the planned setup window if required by local policy, then confirm Core workstations reconnect without rerunning setup.
Connection	Each workstation shows the shared Team connection, not Firebird Embedded/Solo.
Identity	Each person sees the expected display name and role from their own Windows sign-in.
Permissions	Hidden modules, view-only modules, and write-enabled modules match the administrator's settings.
Shared data	A saved record appears to authorized users on module entry or Refresh/F5. Visible BOM/Inventory lists check about every 30 seconds; this is not instant collaborative editing.
Stale-write safety	Users understand that a conflict message means reload and compare; they should not try to bypass it.
Backup task	The server contains the JSBS Core Database Backup scheduled task for 2:00 a.m. and the protected C:\ProgramData\JSBS Core\Backups folder.
Off-host protection	The organization has a documented method to protect database backups and required filesystem document/report folders outside the server's failure domain.

DO NOT TEST WITH CUSTOMER DATA Use a harmless setup record or agreed test procedure. Do not create misleading production orders, inventory movements, or commercial documents merely to prove the connection.

MAINTENANCE

Updates, repairs, and schema coordination

Core 1.6.0 requires schema 23 and Database Installer 1.9.0. Maintain the Team server before updating clients. Replacing the installer executable alone does not upgrade the database.

Application-only Core update

- Users may update Core normally when the release says database change: no and the schema number is unchanged.
- Team workstations may update independently for that application-only release.
- Do not rerun the Database Installer solely because the Core patch number changed.

Core update with a Team schema change

1. **Schedule a maintenance window.** Have every Team user save work and close JSBS Core.
2. **Confirm the matched versions.** Read the target schema and required Database Installer version in the Core release guidance.
3. **Update the database first.** On the server, run the matching Database Installer and choose Repair or update server. It creates and restore-verifies a backup before migrations.
4. **Update every workstation.** While users remain out, install the matching Core release on all Team workstations.
5. **Reopen and verify.** Connect, confirm the Team status, and perform the normal focused read/write checks.

SCHEMA MISMATCH Core stops before opening an incompatible Team workspace. Never edit the schema version, rerun old migration files, use an older Database Installer, or point the Team installer at a Solo database.

PROTECTION

Backups and security responsibilities

Daily backup	Runs at 2:00 a.m. under Windows SYSTEM, creates a logical .fbk, restores it to a temporary database, and removes the temporary verification database after success.
Pre-maintenance backup	An existing Team database receives a verified safety backup before repair or supported schema maintenance.
Backup scope	Database-stored records and embedded attachments are included. Separate document libraries, saved PDFs, report folders, and exported files require their own protection.
Failure domain	A backup kept only on the same server is not sufficient protection against device loss, theft, ransomware, or disk failure. Follow an approved off-host/offline retention policy.
Connection key	Treat it as a shared database password. Restrict it to authorized Core users and rotate/recover it only through an approved maintenance process.
Firewall	Expose only the selected TCP port on trusted Private/Domain networks. Do not publish the database service to the public internet.
Live database	Never copy an open .fdb file. Use logical backup/restore and a planned maintenance window.

RECOVERY IS A PROCEDURE Keep the Database Installer, current Core version information, server/port record, protected connection details, verified backups, and named recovery owners together in the organization's continuity plan.

TROUBLESHOOTING

Common installation and connection problems

Administrator approval required	Close the installer, sign in with or provide a Windows administrator credential, and reopen it.
Database folder rejected	Choose an empty folder on a local server disk. Do not use a network share, mapped drive, drive root, or folder containing unrelated files.
Port already in use	Choose another port such as 3051, rerun setup, and use that same port on every workstation.
Cannot reach server	Confirm the server is powered on, the name/IP and port are exact, both computers are on the trusted network, and the Private/Domain firewall rule is enabled.
Connection key rejected	Copy the complete key again from the server result. Remove accidental leading/trailing spaces and do not substitute an example key from this guide.
Workspace access refused	Ask the administrator to add the exact Windows identity, keep it active, and grant appropriate View permissions. Close and reopen Core afterward.
Wrong user or role	Compare the Windows identity with the saved workspace account. Domain and local identities that share a username are still different accounts.
Team database is older	Close all users and run the Database Installer version named by Core on the server before updating/reopening every workstation.
Team database is newer	Leave the server unchanged and update the older Core workstation to the matching release.
Different database folder shown	Do not use repair/update to relocate an installed database. Stop and use a separate verified maintenance plan.

QUICK REFERENCE

End-to-end Team setup checklist

1. **Server selected** 64-bit Windows host, trusted network, reliable availability, local database disk.
2. **Exact administrator identity recorded** The Core workstation identity, not merely the server login suggestion.
3. **Database Installer run as administrator** Approved download, current matched version, local empty folder, port, firewall option.
4. **Ready details protected** Server name/IP, port, JSBS_CORE alias, and generated connection key stored securely.
5. **First administrator connected** Team-capable Core license activated; Company server selected; identity and Administrator role confirmed.
6. **Every workspace user added** Exact Windows identity, display name, active state, administrator state, and module permissions.
7. **Every workstation connected** Approved Core installer and license; same host, port, and key; Team status and real access verified.
8. **Backups covered** Scheduled verified backup confirmed; off-host database and separate document/report protection assigned.
9. **Update owner assigned** Named administrator reads compatibility guidance and coordinates schema-changing maintenance.

SAFE HANDOFF Give ordinary users only the connection details and steps they need. Keep server administration, backup locations, recovery procedures, and elevated credentials with the designated administrators.

Support information to record

Database host / port	_____
Database Installer version	_____
Core version / schema	_____
Primary / alternate owner	_____
Last verified backup / restore test	_____