MANAGEMENT OF USER ACCESS RIGHTS IN JIG DASHBOARD

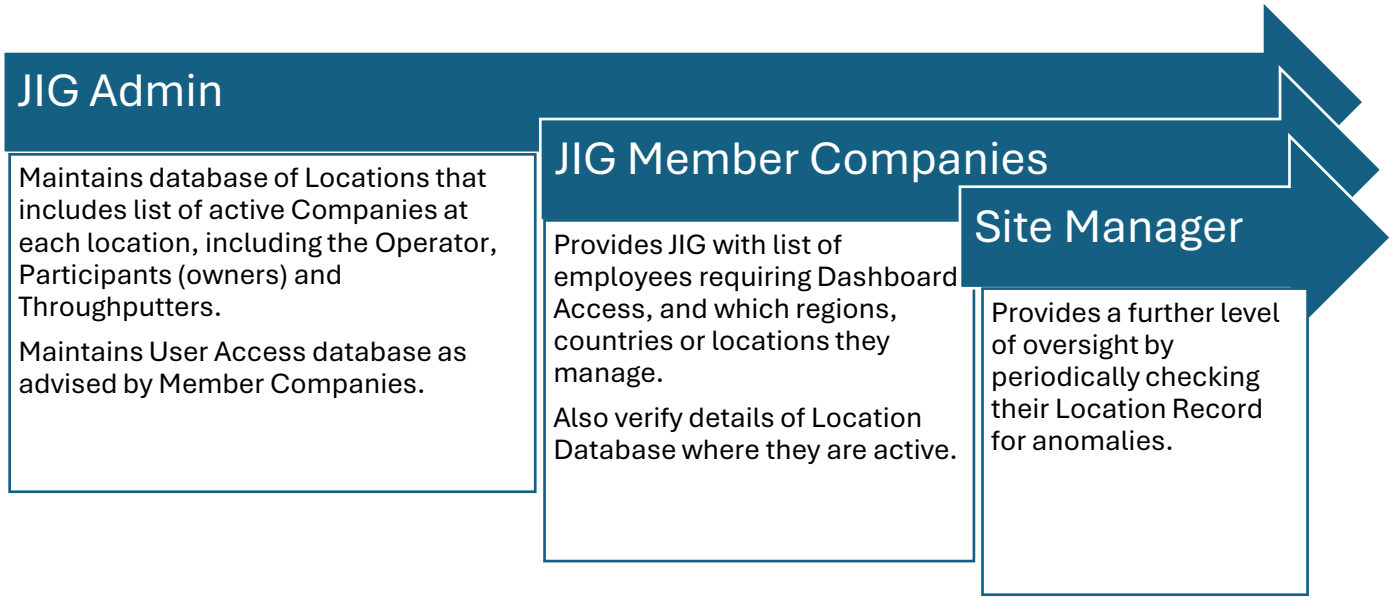
28th March 2025

The new JIG Dashboard tool, launched in 2025, is designed to help Users and Site Managers to manage their operations operating to JIG Standards. It stores key operations data submitted by participating locations, which is analysed prior to being made available to Users who are authorised to view data from the location concerned.

The Dashboard has been designed to ensure the security and ongoing confidentiality of data hosted by JIG. This information document provides further details about Access Rights management and how JIG Member Companies' data is managed and protected.

Three Levels of Access Rights Management:

Security of Data is achieved by JIG Admin, JIG Member Companies and Site Managers working together to ensure that JIG Member Locations and Company Users' geographical profiles are accurate and applied correctly.

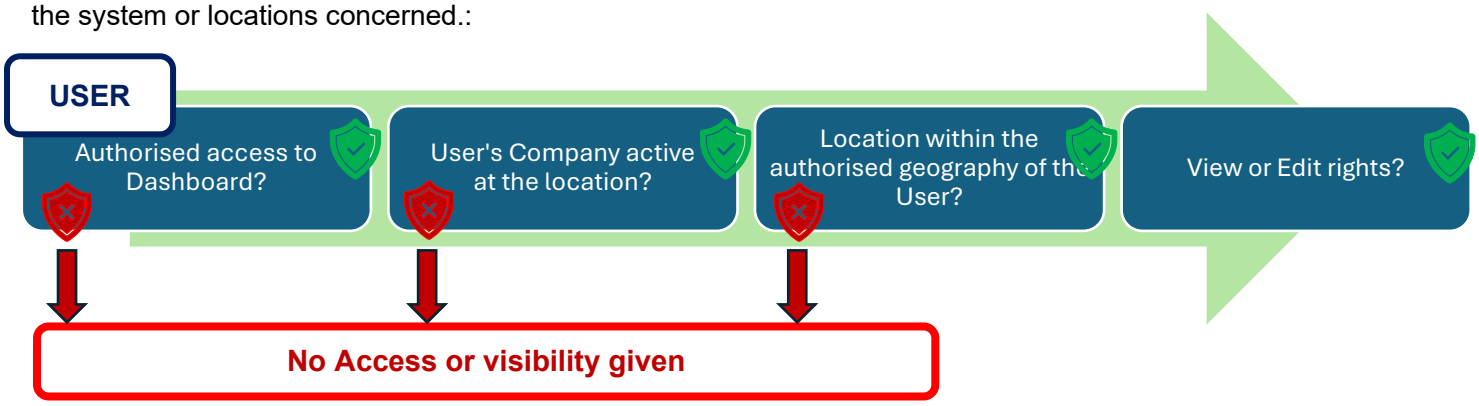


A single Database is used to Manage Dashboard, Tarbox and JITS. The JIG Member companies also decide which of those systems their employees require for their daily work. Access to Dashboard, for example, does not automatically confer rights to the Tarbox or JITS systems. The Site Manager view indicates which of the 3 systems an authorised user for that site has access to.

User Permissions and Data Access:

1. User permissions:

As indicated above, User permissions are managed individually for each system and verify that the User Company is present at the Location concerned, that the User has been authorised by its company for that Location, and checks if the User has "View" or "Edit" permissions. If a User does not meet all the criteria, no access is given to the system or locations concerned.:



The prevailing access rights philosophy for "authorised Users" is to geographically limit user access strictly to what is required to carry out their duties. So even if a User's company is active at a given location, that location is only visible if the User also has corresponding access for the airport, country or region.

2. User Profiles :

There are 4 principal user profiles in the system:

- Member Coordinator: There is one per JIG Member Company. They validate all Users and access requests from the Company. Member co-ordinators have "View" rights to all Locations at which their company is active.
- Site Manager / Area Manager: Site (Location) Managers belonging to a JIG Member Company who manage a single site (SM). They only have access to a single Location and can EDIT the operational data for their Location only. Typically, HSSE Data entry, Bulletin implementation, Governance Checklists. They cannot edit the lists of active Users or active Companies. Any anomalies are sent to JIG for adjustment in the database. Area Managers are "Site Managers" who provide oversight to multiple locations, rarely more than five, and have the same permissions as Site Managers.
- Member Admin: Have View rights only in Dashboard to Locations authorised by their company and have some additional functionality in JITS only. Their access typically ranges from 5-20 Locations.
- All other Users: Have View rights only in Dashboard to Locations authorised by their company. Some individuals with Central Support roles may have view access to all of their Companies' locations, though typical Users have access to a single Country or Region.

User Profile Summary				
PROFILE	1-5 LOCATIONS	COUNTRY	REGION	GLOBAL
JIG ADMIN	VIEW AND EDIT			
SITE/AREA MGR	VIEW & EDIT(1)			
MEMBER CO-ORDINATOR	VIEW ONLY			
MEMBER ADMIN	VIEW ONLY			
OTHER USERS		VIEW ONLY		

Typical View/Edit rights – LIMITED to locations where their company is present and MC approval.

(1) May edit Operational data for their Location only.

3. Access to raw data:

Access to modify raw data in the system is limited to JIG Admin and to Users who have Edit rights for a Location. It should be noted that although site managers enter Working Hours and Fuellings data to enable calculation of HSSE KPIs, this detailed data is not visible in the front-end user interface for View-only users. As stated above, Site and Area Managers may change and update their Operational data, but have no rights to edit the data managing Location Configuration, Companies and Users.

Some operational data is available for Users to Export for analysis, though this is always limited to the Locations they are authorised for and the data that is seen on-screen by View-only Users.

When the new Tarbox environment is developed, some general Users will be given authorisation to upload new Tarbox Agreements for certain locations. This will give access to raw data relevant to Agreements, but only in the Tarbox environment and only for authorised locations.

Data Controls:

JIG has a policy of multiple authentication of data in the system. The addition of a new location will typically be verified with the Operator and at least one other active Company. Changes to location data are similarly cross-checked with the Site Manager prior to implementation. Company Users may register themselves online for website use, but all requests for Dashboard and Location access have to be validated directly with JIG by the Company's Member Coordinator.

Every year the system identifies inactive Users for removal from JIG Systems. JIG also requests Member Coordinators and Site Managers to review their Company/Location details and the respective list of Authorised Users every year.

Cyber Security:

Dashboard is hosted on the main JIG Website, that uses up to date software and protocols to protect data and Users. All Users need to update their passwords every year, and Dashboard access is not available to non signed-in users. Furthermore, Dashboard is not accessible the public website menu.

The system access protocol for JIG Admin, because they have access to raw data, is managed using 2-Factor Identification to provide an additional level of security.

The new website platform and environment launched in 2021 has robust security protocols. Our website providers conduct periodic penetration tests to check for weaknesses and have recently deployed reinforced front-end protection to counter potential activity by bots.

We rely on information from Locations and Member Companies to ensure that the Location and User database is accurate, without which we cannot effectively manage access and keep your operational data secure. Please report any incorrect data that you see. Please also ensure that any requests for new locations, or changes to existing ones, are correctly documented.

If you need clarification about the Dashboard set up, your User rights, Company or Locations, please do not hesitate to ask. dashboard@jig.org

28th March 2025