Jigsaw Access Policy

Last Update:

August 2025

Introduction

Jigsaw provides excellent client service while maintaining the security posture our risk-conscious clients need.

Jigsaw's default access policy is outlined within this document.

Jigsaw Architecture

Clients' data in the Jigsaw application can be accessed via two methods:

1. Using the Jigsaw web app. (e.g., logging in to https://firmname.jigsawcreate.com)
2. By directly interacting with the client's Jigsaw database.

Accessing the Jigsaw Web App

Access to the Jigsaw web app requires authenticated login. Users may authenticate using Single Sign-On (SSO), a temporary login token, or a manually configured username and password. Jigsaw recommends using SSO authentication when possible.

When a client requests support that requires access to their Jigsaw web app, the Jigsaw support representative must first obtain written permission from the client team member making the request.

After client permission is received, the representative submits an internal access request. This request is reviewed and approved by a Jigsaw approver, selected from a list of authorized approvers maintained internally by Jigsaw.

Once both the client and a Jigsaw approver have granted approval, the representative is issued temporary access via a time-limited login token. This approval remains valid until the earlier of (i) the point at which the support query is resolved; or (ii) 14 days from the date of the approval, unless the client specifies a different duration. All access is logged.

Clients may also add Jigsaw employees directly to their instance by creating user accounts with manually configured login credentials. This is often done to enable ongoing support or training. Responsibility for managing and disabling these accounts rests with the client.

Accessing the Jigsaw Database

Jigsaw is hosted in Microsoft Azure. Each client's Jigsaw data is stored in a unique SQL database dedicated to that client.

In some cases, resolving a support request may require direct access to the client's database. In such cases, the Jigsaw support representative must first obtain written permission from the client team member making the request.

Once client permission is received, the representative submits an internal access request. This request is reviewed and approved by a Jigsaw approver, selected from a list of authorized approvers maintained internally by Jigsaw.

Only designated members of Jigsaw's development team have the technical ability to access and interpret client databases. Once both client and Jigsaw-side approvals are granted, temporary access

is issued to a development team member for the purpose of resolving the support issue. This approval remains valid until the earlier of (i) the point at which the support query is resolved; or (ii) 14 days from the date of the approval,unless the client specifies a different duration. All database access is logged.

Approvals

If a client would prefer to name specific approvers who can provide permission to access their Jigsaw instance (web app or database), this can be implemented. One of the key benefits of partnering with Jigsaw is our excellent client service. Adding a layer of centralized approval to support queries will extend the time needed to remedy them.

Access to Test Instances

A test instance is a non-production Jigsaw instance provided to the client for the purposes of testing features, workflows, or configurations without impacting live data.

Clients typically do not — and are not expected to — store sensitive or confidential information in test instances due to the experimental and collaborative nature of such instances. If any such data is included, clients are requested to inform Jigsaw in writing so that appropriate controls can be applied.

If a client has a dedicated test instance, access restrictions outlined in this policy do not apply to that instance. Test instances are considered non-production systems, and Jigsaw team members may access them for administrative purposes including but not limited to troubleshooting, feature validation, testing, and training.

Special Procedures

Some processes discussed in this document can be amended as needed to comply with client requirements.

If you have any questions about this Access Policy or would like to discuss special handling, please reach out to either your Jigsaw Customer Success Manager or support@jigsawcreate.com.

Note that Jigsaw may access a client's Jigsaw instance for the purpose of maintaining a client's compliance with the licensing terms in accordance with the EULA without the written permission of the client.

A Note on Jigsaw Documents

Within Jigsaw, users create documents accessible **only** to authenticated users within their firm's instance. By default, new documents are set as **Public**, meaning they are visible to all authenticated users within that instance—but not externally. Document owners can manually restrict visibility by setting documents as **Private**, making them accessible exclusively to designated users.

This default-open approach aligns with how most firms manage document collaboration. Administrators can, however, change the default visibility to Private via the admin panel.