Security Features

Cloud Version (iPaaS)

- Cloud Workflow (iPaaS) operates on AWS cloud platform. It applies industry best practices to secure application access control and operation.
- All stored passwords are encrypted with industry standard encryption algorithms.
- All Web communications - with connected applications - comply with HTTP/S 256 bit encryption standards.
- No customer data is stored on our platform. Data is processed in-memory. There can be instances where data could be written to account specific log files.
- iPaaS iPlatform s annually scanned for security by our partnering apps like Salesforce, Intuit and Microsoft.

On-Premise

- The On-Premise version of iPaaS can be downloaded and installed from mydbsync.com. The installation is available for Windows (**.exe) or Linux (**.zip) file.
- The On-Premise version of iPaaS is built to run it's user interface, on top of Tomcat web server.
- All configuration for On-Premise version of iPaaS projects are stored in local file system.
- All stored passwords are encrypted with industry standard encryption algorithms.
- All Web communications - with connected applications - comply with HTTP/S 256 bit encryption standards.
- DBSync License check occurs at every run using HTTP/S 256 bit calls to DBSync License servers. This call can be avoided by installing a local license file (Ask for installing a local license file from your implementation engineer).

FAQ

Q : Where is iPaaS Cloud version running?

A: DBSync iPaaS runs on Amazon AWS. It provides state of the art data center and is fully security compliant. For more information logon to Amazon.com.

Q: Do DBSync iPaaS either - On-Demand or On-Premise - version store data on their server for the applications that are being connected ?

A: No. No data is stored in any applications that are being connected using our platform. We only store configuration with industry standard encryption algorithm to facilitate data flow between source and target application.

Q : What logging is in place for iPaaS?

A: DBSync generates configuration specific logs (Projects) under a "log" directory and Tomcat log files. The "log" file is located under the installed directory but can be switched to another location through setup. The information logged is related to the progress and errors. No confidential data is written to the logs.

Q: What kind of transport level security is covered?

A: This is done via SSL. For more information logon to transport layer security.

Q: How secured is DBSync - to prevent tampering, or other unauthorized modifications, to its configuration?

A: DBSync is built on Apache Tomcat/Java. Application access control is managed by our Global License and User Management. Admins or Users do not have direct access to stored configuration files.

Q: How does DBSync authenticate applications that need to be integrated? And, how SSL/HTTPS confirmation is enforced for authentication/data transfer?

A: DBSync uses Custom Web services to authenticate and communicate with third party applications. It uses HTTP/s protocol while communicating with these application via web.