Security Architecture and FAQ

Security Architecture

DBSync Cloud Replication provides a fast and easy way to replicate Salesforce in your local database.

Security Highlights

- DBSync Cloud Replication is a 100% Java application.
- The application can be downloaded and installed from mydbsync.com product site. The installation is available for Windows (**.exe) or Unix/Linux (**.zip) file.
- The application is built to run its user interface on top of Tomcat.
- The application does not provide any in built User Security model. End users can implement security based on Security (http://tomcat.apache.org/tomcat-6.0-doc/realm-howto.html) or Spring Security (http://projects.spring.io/spring-security/)
- All configuration for profiles are stored in local file system <<install-dir>>/dbsync-repl/WEB-INF/db directory
- All passwords stored are encrypted with industry standard encryption algorithms. The encryption seed can be changed once installed.
- The following are the entities and passwords that are encrypted –
    - Local license file (*.lic)
    - http Proxy Password
    - Salesforce Password
    - Database Password
- All Web communications with Salesforce comply with Salesforce HTTP/S 256 bit encryption standards.
- All communication with local database is performed using JDBC protocol and supported JDBC drivers.
- 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.
- The application can run standalone or embedded along with other application. Most common operating model is to use Batch Interface in Solaris/Unix environment and / or Web App on Windows/Linux/Unix environment.

FAQ

- Where is dbsync running? On database server at our IT center? Separate/dedicated server at our IT center? Other?
    - *DBSync runs in your IT Center. While it is recommended that you create a virtual machine to run the application, it can co-exist with other application. The application runs on Java in its virtual Java process space and will not interfere with other application.*
- Does DBSync transfer and/or storage of SFDC credentials? If true, this is a security issue.
    - *DBSync **does not transfer client data or store any of their SFDC credentials**. The only communication it has with its servers are for license checks. These checks can be avoided by installing a local license key.*
- DBSync configuration must prevent transfer of data to other databases including un-related orgs at SFDC or other servers inside or outside of our centers. How is this accomplished?
    - *The end user sets up connection to its database. The Engine reads data from one source, maps and translates it in memory to push it to target or destination. At no point the data is written to disk or routed to another destination.*
- How does DBSync authenticate to SFDC? Confirm SSL/HTTPS is enforced for authentication/data transfer?
    - *DBSync uses Salesforce SOAP services to authenticate and communicate with Salesforce. It uses the required HTTP/s and encryption required as required by Salesforce API's.*
- How is DBSync secured to prevent tampering or other unauthorized modification of its configuration?
    - *DBSync is built on Tomcat and Spring framework. While out of the box, it does not come with user management, one can easily*

implement Tomcat Realm Security or Spring Security to implement their security. It is also recommended that this server be accessible only through approved IP ranges to further protect access to the server. If you are running the application in batch mode, you do not Tomcat Server to be running once its setup. This will further secure any web access to your install.

- Is any information about Client instance (rules, login credentials, etc.) stored elsewhere other than Clients own server running DBSync processing?
    - *DBSync does not store any information about the client Salesforce configuration or data in any other server that the ones installed or connected.*

- DBSync Audit trails - Where are they? What is logged? How are logged protected? Is any confidential data contained in the logs?
    - *DBSync generates configuration specific logs (Profiles) under a "log" directory and Tomcat log files. The "log" file is located under the install directory but can be switched to another location through setup. The information logged is related to the progress and errors. No confidential or data is written to the logs.*