Best Practices for Securing Personal Data

In support of enhanced data protection initiatives, consider implementing these recommendations.

Database Encryption

One way to encrypt the InterBase database is the volume-based NTFS method. Make sure you have the recommended server requirements before encrypting the database.

- Encryption should be configured on the server where the InterBase service is running and where the InterBase database files are located.
- Create a functional Windows login account with local admin rights.
- Configure the InterBase server and guardian to run as that functional account.
- Stop/Restart InterBase and connect to a database via IB Console to confirm InterBase is working correctly.
- The database files cannot be active while the encryption is being enabled, so stop the InterBase Service.
- You can encrypt a single file or a folder. The process is basically the same either way. First, select the file or folder to be encrypted via File Explorer.
- Right-click on the file or folder and select properties.
- Click on the "Advanced" button toward the bottom of the form.
- Check the box labeled "Encrypt contents to secure data" and click OK.
- Click OK on the Properties dialog.
- If you're encrypting a folder, you'll see an additional dialog "Confirm Attribute Changes"; if you want all the files in the folder encrypted as well, then check the radio button that says, "Apply changes to this folder, subfolders and files" and click OK.
- You'll see a progress indicator while the file or files are being encrypted. The time it takes to encrypt depends on the speed of the PC and the size of the file.
- Once the encryption process is done, the file or folder will show in the file list as green instead of black, to indicate encryption enabled.
- Restart InterBase.
- Connect to an encrypted database via IB Console to confirm InterBase is working correctly.
- Reversing encryption is basically the same process, except you uncheck the "Encrypt contents to secure data" box.

Securing the InterBase client-server connection

Below is the link to Embarcadero's site on how to secure the InterBase client-server connection:
http://docwiki.embarcadero.com/InterBase/2017/en/Setup_OTW/SSL_and_InterBase

Securing the TramsAppServer connection

For Trams Back Office/ClientBase Windows Remote connection:

- To enable RSA encryption, create a DWORD registry key hkey_local_machine\software\wow6432node\trams\appserver\encryption and set to 1.

For Trams Invoice History App:

- create a STRING registry key hkey_local_machine\software\wow6432node\trams\appserver\SSLCertificatePath and set to path to certificate file (.crt).
- create a STRING registry key hkey_local_machine\software\wow6432node\trams\appserver\SSLKeyPath and set to path to key file (.key). It may be possible to just use a .crt file (need to verify).
- If using a non-standard SSL port (other than 443), create a DWORD registry key hkey_local_machine\software\wow6432node\trams\appserver\WebServerPort and set to desired port number.
- Start TramsAppService.
- Open link to TramsAppService (e.g. https://localhost/) in FireFox ->Advanced->Add Exception>View->Details->Export and specify path to save certificate file. (this step it for retrieving .crt file that was used to configure TramsAppService).
- Go to folder of Java installation that is used by Sabre Red Workspace – default location is: "c:\Users\<userName>\AppData\Local\Sabre Red Workspace\Common\binary\com.oracle.java.jre.win32.x86_1.8.0.025" -> <Sabre Red Workspace Java path>
- Open bin folder.
- Start command line as administrator (inside <Sabre Red Workspace Java path>\bin).
- Run "keytool -import -v -trustcacerts -alias TAS -file <path to *crt file> -keystore "<Sabre Red Workspace Java path>\lib\security\cacerts" -keypass changeit -storepass changeit" (example: keytool -import -v -trustcacerts -alias TAS -file c:\praca\tiha\tramsappserver.crt keystore "c:\Users\sg0891845\AppData\Local\Sabre Red Workspace\Common\binary\com.oracle.java.jre.win32.x86_1.8.0.025\lib\security\cacerts" keypass changeit -storepass changeit)
- Press 'Y' when asked if 'Trust this certificate'.
- Start Sabre Red Workspace.
- Configure TIHA to use https connection to TramsAppService.

Enable Embedded User Authentication (EUA) on the database

EUA-enabling the InterBase database allows benefits from the new password management features of setting password strengths, setting password expiration dates, as well as users being able to change their own passwords. Please refer to Password Protection section of the help files on the requirements and steps to EUA-enable a database.

Troubleshooting files for service incidents

When reporting issues regarding ClientBase Merge to PNR, PNR Import, Live Connect, or Trams Back Office GDS Interface, our support team requests you to save the PNR, IUR or log files. These files contain personal data. Make sure you delete these files on your machine after sending it to our support team. We will delete our copies within 28 days.

Please contact Trams and ClientBase support for any assistance.