

Syncaphone Security Model

Can Syncaphone Protect My Data?

Yes. It was decided to implement a custom secure connection using Advanced Encryption Standard (AES) with 128 bit symmetric encryption keys. While Syncaphone does not support SSL, it supports AES encryption on both MIDP 1.0 and MIDP 2.0 devices and does:

- Provide encryption for authentication,
- Provide encryption for data transfer,
- Allows use of standard port 80 or port 8080, and
- Permits the use of a secure "poison pill".

Syncaphone Security Architecture

Syncaphone Server

The server part of Syncaphone is a usual web application deployed on the Servlet/JSP container of the Tomcat server. Tomcat is a part of the GroupWise architecture on NetWare 6.x and Linux. Syncaphone server uses the same web application as GroupWise WebAccess and Web Publisher. The only process that can be triggered outside of Tomcat is a small Java application for restarting Tomcat (this option is included in the Syncaphone web administration panel). For the Syncaphone server, the source of the GroupWise data is the GroupWise WebAccess application. Thus Syncaphone uses GroupWise WebAccess as a "conduit" into the GroupWise System (Domains and Post Offices supported by GroupWise WebAccess). The transfer of data between the Syncaphone client and the Syncaphone server is protected using AES encryption. The exchange of data between the Syncaphone server and the GroupWise WebAccess Application server is not secured. The reason is simple - it is the communication between two applications running on the same physical server platform, usually using the 127.0.0.1 network interface. Data transferred between GroupWise WebAccess and the GroupWise Domains and Post Offices is protected by GroupWise.

Syncaphone Secure Connection

The most sensitive part of the data transfer is between the Syncaphone client and server. The secure communication between the client and server employs the following technology:

- Data is encrypted using Advanced Encryption Standard (AES) 128 bit symmetric encryption keys,
- A default encryption key is used only once - when the client attempts to connect and login to the Syncaphone server part.
- The default encryption key is generated during the first startup of the server application and it is unique to that installed Syncaphone server. The default encryption key makes use of some parameter's (like the date of the first server startup and the IP address of the server) to ensure that no two Syncaphone servers will use the same default encryption key. Once generated, the Syncaphone server attaches its default encryption key to the client download package. A user must download the client application from the "correct" Syncaphone server - it is impossible to use a client application downloaded from another server as there will be a mismatch between default encryption keys.
- When a client attempts to connect to a Syncaphone server, and the key is approved by the Syncaphone server. It is used to secure the username and password. Once authentication is complete, the default encryption key is not used anymore.

- Any request encrypted with the "incorrect" key is rejected and a -125 error is visible at the client side.
- The GroupWise password of the users exchanged with the server only once.
- For normal data transfer between the client and server uses a "quasi randomly generated" encryption key for each for each request/response. The "quasi randomly generated" encryption key never contains the user password - only some of the password characters are used for generating the key.

Is Encrypted Data Transfer Fast?

Yes. The limited computing power of mobile devices and limited bandwidth of most mobile networks were the reason to implement a new, fast and very efficient "Syncaphone communication protocol". This protocol is customized to Messaging and Collaboration data types and is embedded inside the http protocol. It utilizes highly efficient content delimiters - and in fact it uses binary format of data. The "Syncaphone communication protocol" makes encryption process faster, especially on the mobile devices.

Syncaphone "Kill Pill"

The administrator of your Syncaphone server has the option of disabling the client application remotely. If a mobile device is lost or stolen, the administrator can "disable" the device in the Syncaphone admin web pane). The next time the client application attempts to connect and login, the Syncaphone server will issue a "kill pill" which will erase all Syncaphone data stored on the device and disable the client application (no command will exist except the EXIT command).