2014

LBCOM

http://www.liveboxcloud.com

LiveBox Srl does not release declarations or guarantees about this documentation and its use and declines any expressed or implied commercial or suitability guarantee for a specific purpose. LiveBox Srl reserves a right to review this publication and to make changes to the content, anytime, without any obligation to notify it to any person or entity regarding revisions or changes.

In addition, LiveBox Srl does not release declarations or guarantees about any software and in particular does not recognise any expressed or implied commercial or suitable guarantee for a specific purpose. LiveBox Srl reserve one's right to review this publication and to make changes to any LiveBox software part, anytime, without any obligation to notify any person or entity about such revisions or changes.

LiveBox is a private cloud software that allows you to store, share and edit data stored in a corporate datacenter offering a high security level. LiveBox is a multiplatform system accessibile from every mobile and remote device that guarantees business continuity and protects corporate files at all times.

For further details regarding the LiveBox platform functionality and the use of its applications we ask you to refer to our web site: http://www.liveboxcloud.com and to the technical documentation contained therein.

LiveBox Support Team

Index

1. LIVEBOX, A PRIVATE FILE SHARING 4

2. COMMUNICATION 5

2.1 XMPP 5

2.2 PUSH NOTIFICATIONS 5

2.3 MESSAGING 6

2.3.1 Message chronology 6

2.3.2 Off-the-Record Messaging 6

1. LIVEBOX, A PRIVATE FILE SHARING

LiveBox is a private file sharing platform with a client/server architecture. The server is located within the customer infrastructure, ensuring privacy and security of the data.

Having an internet connection with a public IP (or recorded on a dynamic naming service) it is possible to guarantee accessibility from remote locations. It can be accessed from standard compatible browsers HTML5 (IE 10, Firefox, Chrome, Opera, Safari), from OS Android systems (4.x), from iOS systems (from 6.x), from Windows systems (from XP SP3, 32 bit or 64 bit), from Mac OSX (>= 10.7). During 2014 support for Windows Phone 8 will become available.

The two key paradigms that lead our development platform are:

- Installation and access using your existing hardware infrastructure.
- Sharing contents, in a private and secure way, without relocating files.

2. COMMUNICATION

LiveBox has a module that you can be purchased separately that manages the communication between users supplying instantaneous and push notification. Additionally, supporting third party IM servers, for example Facebook, Google Hangout e CISCO. This is made possible as it is based on the XMPP (RFC 3921)[1] protocol.

2.1 XMPP

All open messaging and presence protocols are grouped under the XMPP name. LiveBox system uses the XMPP protocol to develop a private messaging platform (because it is resident on the clients infrastructure servers), and secure (because it runs on an encrypted channel with a web certificate; accessed through user credentials and further encrypted with a PIN code chosen by the user). No competing system has such a strong authentication level or encrypted conversation system among users.

This platform fosters collaboration among LiveBox users that get a communication instrument, with exchange and file sharing functions, without increased network load or storage space requirements. This allows publication of corporate projects across working groups without spamming mail servers, internal or external.

2.2 PUSH NOTIFICATIONS

LiveBox sends messages to clients using XMPP to notify system events, as folders creation, sharing etc.

This solution is actively used by the desktop client and by mobile clients: agents use this policy to optimize synchronization with the server, reducing network throughput and payloas; mobile devices use push notification to receive human readable notifications with updated information relating to the shared data.

[1] http://www.ietf.org/rfc/rfc3921.txt

2.3 MESSAGING

iOS and Android applications use the XMPP protocol to implement an instantaneous messaging service (chat).

Messaging services imrpove sharing processes, allowing drag and drop of content across folders and files with IM Contacts.

2.3.1 Message history

Messages exchanged in an IM conversation are saved on client and server through the implementation of an XMPP Extension (XEP-136[2]) Message Archiving. These will be synchronized across devices using the archiving backend on the IM server.

2.3.2 Off-the-Record Messaging

The chat implementation on mobile devices includes the OTR[3] protocol, that allows asymmetric encryption of exchanged messages in 1-1 conversations using keys generated on the fly with a Diffie-Hellmann[4] exchange. This feature is activated after a user requests encryption in the conversation screen; in this case, a couple of private-public keys will be generated on both devices; the public one will be sent to the user with which the encrypted session is being launched and viceversa. Both keys will be used to generate a third key (called a shared key) that will be later used to encrypt communications with a symmetric cryptography schema.

This type of conversation is not saved on the device, or on server, and leaves no tracks, guaranteeing user privacy and discretion.

[2] http://xmpp.org/extensions/xep-0136.html

[3] http://www.ietf.org/rfc/rfc3526.txt

[4] http://www.ietf.org/rfc/rfc2631.txt