FixMe.IT
by Techinline

# FixMe.IT Security

An in-depth look at FixMe.IT’s architecture & security features

FixMe.IT by Techinline

# Table of contents

## Target audience

This document is aimed at IT business owners and network administrators, who would like to have a detailed look at the architecture of FixMe.IT before purchasing a license and deploying the software. In case you do not consider yourself to be part of the target audience, please see the Security section of our website to get a general overview of the product's security features.

Please feel free to share the information below with your customers to eliminate potential security and privacy concerns.

## About FixMe.IT & Techinline

Techinline Ltd. was founded in 2006 by a group of highly experienced technology professionals with the mission to provide businesses and home users alike with a powerful, easy-to-use and cost-effective remote support application. Techinline's headquarters and sales offices are based in the United Kingdom and Canada.

FixMe.IT (previously known as Techinline Remote Desktop) is a remote desktop application that provides instant connections between remote computers and allows IT professionals to quickly view, diagnose and resolve technical issues anywhere in the world. FixMe.IT is currently used and trusted by thousands of users from over 63 countries.

## Terminology

**Expert:** A technician using FixMe.IT to provide remote technical assistance to end-users.

**Client ID:** A unique 6-digit number generated by the FixMe.IT Client application that allows the Expert to send a connection request to the remote user.

**Remote Desktop Toolbar:** A feature panel in the FixMe.IT Expert application that becomes available upon starting the remote control operation.

# Introduction to FixMe.IT security

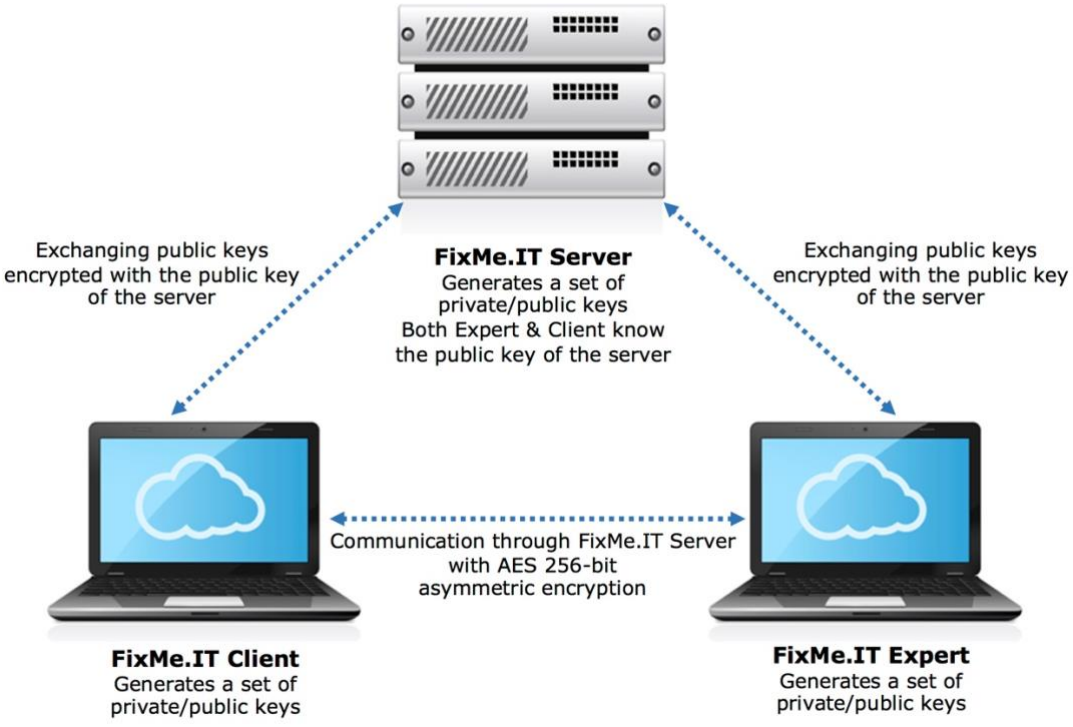
Techinline FixMe.IT is a web-based service that delivers a way to remotely connect to Windows computers and tablets in a matter of seconds. FixMe.IT allows the remote user to request technical assistance from the Expert by downloading a temporary client application via browser and then provides the Expert with the ability to start a remote support session to view and control the remote user's desktop. Initially, no software installation is required on the remote user's side.

Every support session is fully protected with industry-standard 256-bit SSL/TLS encryption. This means that no screen captures, commands or files can be intercepted by any third party. Support sessions must be approved by the remote user before the Expert can connect to their computer.

The only session information that is stored are Session Start/End Time, Notes, and Client Name. FixMe.IT does not store chat logs, system messages, transferred files and data, etc. This information is transferred only between the Expert and the remote user and leaves no footprint anywhere in the middle. This means that there is no risk of transferring sensitive information as it will be entirely disregarded from all points at the end of the session.

All remote desktop operations can be recorded with a built-in video session recording tool available in the Remote Desktop Toolbar.

The image below provides a schematic overview of the FixMe.IT architecture and all key communication processes.



## Expert authentication

FixMe.IT Experts are authenticated using an email address and a password, which is protected with salted cryptographic hashing and stored in an encrypted database.

Besides that, strict password policies that require 8-30 characters and must include both upper and lowercase symbols are applied to Experts. A strong password must not be the same as the email address or the name of the account holder.

## Protection of remote user's PC & data

FixMe.IT utilizes permission-based access control model, which means that the remote user is always in control of what's happening on their end and thereby ensures the highest level of data protection.

All FixMe.IT sessions must be initiated by the remote user. The Expert cannot establish the remote connection until provided with a unique Client ID generated by the FixMe.IT Client application. Besides that, the remote user is always prompted for permission to access their computer before any operation is started.

In case there is a need to setup unattended access on the remote user's computer, the remote user is prompted to grant permission to the Expert and can always abort the unattended connection by clicking on the FixMe.IT icon in the Windows system tray and choosing the corresponding option.

If the remote control operation has been authorized, the remote user can always see what's happening on their screen and can terminate the session at any time.

The Expert cannot alter local security or any other vital settings unless provided with the remote user's Windows credentials.

## Generating Client IDs

Each Client ID is automatically generated, unique, and is deemed active until used by the Expert to start the remote support session. The same Client ID cannot be reused, which means that a new Client ID must be generated each time the remote user requires assistance.

# FixMe.IT communication security features

## Starting a session

FixMe.IT servers determine the optimal type of connection each time a new session is being started. After the handshake through the FixMe.IT servers, a direct HTTPS connection is established between the remote user and the Expert.

Whether the remote user or the Expert are located behind a firewall, proxy server, or NAT, FixMe.IT guarantees a stable remote connection in any environment. The Expert does not need to configure any ports to start a FixMe.IT session.

## Session data encryption

Every FixMe.IT session is fully secured with the TLS 1.2 protocol using 256-bit AES encryption. After the SSL/TLS handshake through a dedicated FixMe.IT server, the two remote parties negotiate a final encryption key just between themselves. The FixMe.IT servers route only encrypted data packets and do not have the session encryption key. This means that the data stream between the remote user and the Expert cannot be altered or intercepted by any third party, including Techinline.

All FixMe.IT SSL certificates are issued by the Comodo Group, a leading internet security provider. More information on Comodo Group's SSL certification can be found here: https://www.comodo.com/.

## No background mode

There's no option within FixMe.IT that allows the Expert to run the application in background. Upon establishing a new session, there is always a FixMe.IT icon visible in the Windows system tray (even if unattended access is installed on the remote machine), which makes FixMe.IT unsuitable for secretly monitoring or performing any unsolicited actions on a remote computer.

## Two-factor authentication

Techinline assists customers in meeting all necessary criteria for getting their business PCI- and HIPAA-ready through optional two-factor authentication. The two-factor login process requires the account holder's username and password as well as a virtual token sent via email, which must be provided upon login.

## FixMe.IT server network

FixMe.IT utilizes a secure network of virtualized Amazon and Microsoft Azure servers allowing the use of ICMP and HTTPS. This geographically-distributed server network identifies the optimal connection between the remote parties and ensures that the Expert always works with a genuine FixMe.IT server.

With hardware firewalls and layered mitigation technology built into the architecture along with highly redundant power supplies and 24/7 monitoring, the FixMe.IT server network ensures that all communication between the Expert and the remote user is highly reliable and secure.

## Compliance in regulated environments

FixMe.IT does not process any payments, nor does it collect any sensitive customer or end user data except for session logs (start/end time of session, IP addresses of participants, the amount of transferred data) and Personally Identifiable Information required for billing and accounting purposes.

All temporary information used or transferred during the session is temporarily stored in the server's operating memory without anyone having access to this information. Once the data is transferred from one session participant to another, it is entirely disregarded from the operating memory. Once the session is terminated, all temporary data is entirely disregarded.

Therefore, FixMe.IT's extensive set of communication security features along with its permission-based access control model and optional two-factor authentication make it suitable for supporting clients in organizations subject to HIPAA and PCI compliance.

## Conclusion

As this document demonstrates, the FixMe.IT remote support application provides end-to-end data protection measures that defend all communications against common security threats along with a highly reliable environment for delivering instant remote assistance to customers located anywhere in the world.

## Contact information

Please forward any questions or concerns to the appropriate email address:

For general enquiries and suggestions, website, feedback and other proposals: info@techinline.com

For order quotes, pricing information, product enquiries and personal demos: sales@techinline.com

*You may also contact the Sales Department to learn more about the FixMe.IT remote desktop application. We will be happy to answer any of your questions, as well as provide a personal demo of our software.

For any technical issues: support@techinline.com

For questions or concerns about an existing FixMe.IT account: orders@techinline.com
We guarantee to respond to your request within 24 hours!

You can also contact a live representative regarding any issue:

**Phone:** US & Canada: 1-617-934-2771

United Kingdom: +44 (0)20 8144-7131

**Skype:** techinline

## Useful links

Official website: https://www.techinline.com/

Overview of FixMe.IT security features: https://www.techinline.com/Security

FixMe.IT Support Center: https://docs.fixme.it