FASTPASSCORP

How FastPass is made secure for you

The increasing number of successful attacks on IT infrastructure to breach data security take many forms. Hackers go to great length to breach into WEB-applications to manipulate data or copy data out to suit their purpose.

The only way to prevent hackers from being successful is to use secure software. And as hackers are continuously looking for new ways to breach into software solutions, system protection too is an ongoing process.

For ***FastPassCorp,*** this means that software security starts with the design of the software and all new releases. We continuously follow the threats to systems and improve how we make our solutions secure for customers and users.

This document presents an overview of some of the actions taken by ***FastPassCorp*** to make our solutions secure. We follow the format of listing the common questions we receive and then answering them, thus providing an explanation of how we protect your infrastructure. We hope you will use the list as a general checklist for all your critical applications to check if you can trust that the software you use is protecting your critical data against hackers.

How are sessions protected in FastPass in general?

1. First, FastPass only accepts communication over SSL so all session communication is encrypted.

2. The session is bound to the specific URL, which means, for instance, that it will not be sent to other apps, even on the same server.

3. We change the session on every request—hence, even if an attack succeeded, it is likely that the sessionID would already have been used and changed.

4. By default, the TRACK STATE engine in FastPass knows the pages you can get to at any point, and if you do not arrive on the expected pages, the session is abandoned. Hence an attacked attempting to repost will fail in doing so.

5. The session can be bound to the IP of the end-user—effectively leaving out listening to requests on a session coming from addresses other than the end-users IP.

How and what data is stored about the end-users?

You can find an exact list of what fields we read/write in AD and what we store and how we do it. The list is available in the technical document named "Microsoft AD integration notes". **Contact us to get the list.**

General sensitive information is encrypted using a 256 Bit AES algorithm. For hashing, we use PBKDF2 (RFC2898).

Are security questions safe to use?

Well, while we think they can be safe, generally we think that it would be safer if you follow these guidelines:

1. Limit the questions to ones that are not easy to locate answers for using social engineering techniques, e.g., do not use the question, "What is your mother's name?" etc. Mix up the question types, e.g., the things you prefer, the things you know, or even the things you have (for instance, driver license number).

2. Change the questions every now and then so hackers will not get to know the questions.

3. In FastPass, we lock the users account after 3 wrong answers; this ensures that an attacker will not get further attempts to dig up the answers. After lock-out, the end-user needs to talk to the ServiceDesk in order to open the account again.

4. FastPass makes sure that the answer has a minimum length and that the answers are not the same as the basic protection.

Penetration testing of the software?

A PEN-test results in a certified document where the test results are presented. Based on the report, you can decide if there are any shortcomings that mean anything to your security protection. FastPass is regularly penetration tested by external certified organizations—PCI/OWASP standards are used. The latest report can be provided on request. These tests also cover SQL injections, XSS attacks, etc.

Do you want to see how you can make a successful process for your ***SSPR*** solution?

CONTACT US:

North America : **+ 818 697 2308**
Europe : **+ 45 4810 0410**
info@fastpasscorp.com
www.fastpasscorp.com

FASTPASSCORP

What about hardening the FastPass server?

FastPass has built a hardening package that you can apply to the FastPass installation in order to get the exact same result as in the penetration test report.

Why do you have a captcha?

The purpose of the captcha is to prevent any robotic attacks trying to get usernames.

How do you protect FastPass from man-in-the-middle (MiTM) attacks?

By default, we use SSL, on top of that we also use ViewStateMac on .Net; further, we also have the FastPass TRACK STATE engine. Also, our hardening implements HTTP Strict Transport Security.

How is the PC Windows client protected?

There is a huge number of security features in play here. First of all, the client will refuse to talk to any other sites than the FastPass site it is configured to. It thus refuses to communicate to other sites, and only the needed document types are enabled. Note this also means that you cannot show videos, flash, etc. on the FastPass pages.

Do you want to see how you can make a successful process for your ***SSPR*** solution?

CONTACT US:

North America : **+ 818 697 2308**
Europe : **+ 45 4810 0410**
info@fastpasscorp.com
www.fastpasscorp.com

FASTPASSCORP

Can you have different authentication types per user?

In FastPass, every user group can have different authentications, and also depending on the Network they are connecting from.

For instance, if user A connects from the Internet, they will need Multi Factor Authentication to reset the password, but if the same user attempts to reset a password from the LAN side, a single factor is enough. User B, on the other hand, might only require a single factor even when connecting from the Internet.

Who can access the administrator client?

Administrators belong to a special group. Administrators must have 2-factor credentials for FastPass authentication.

Can passwords or PIN-codes be sent by e-mail?

This is only advisable if the e-mail is secure. Secure e-mail can be configured in FastPass. And only by a time-limited OTP.

Do you want to see how you can make a successful process for your ***SSPR*** solution?

CONTACT US:

North America : **+ 818 697 2308**
Europe : **+ 45 4810 0410**
info@fastpasscorp.com
www.fastpasscorp.com

What about cross-site scripting XSS, does FastPass prevent that?

For all the pages in FastPass, they do not talk to other sites at all! Communication like that is prevented using multiple methods. Should a user attempt to add data to send malicious scripts or HTML to the HepDesk or Admin sites, they will not succeed as input data is escaped, validated, and sanitized.

This is also true for the administrator–hence even the Administrator cannot add javascripts, etc., in the texts in FastPass.

Does FastPass store the end-user's password?

By default, FastPass does not store the end-user's password. FastPass can be configured to store the password either hashed or encrypted.

In that event, it can be used in the Password Policy to ensure the password contains at least 2 different characters to the last password set, etc.