System description for ProcessManager

Introduction

This document outlines the technologies and features used in ProcessManager. It covers our browser requirements, as well as how we keep the hosted version of ProcessManager safe, resilient, and reliable.

Requirements

To access ProcessManager, you simply need a modern browser. We currently support newer versions of Chrome, Firefox, Safari and Edge. While older versions will most probably work, only the two most recent versions are officially supported.

Please note that the official support for Edge only covers the modern Chromium-based version. The legacy EdgeHTML-based version will probably work, but we do not support it, and we do not test it.

All document file types should be supported in ProcessManager. If you experience issues with a certain document or document type, please contact us at tech@process-manager.dk. The maximum size of uploads is currently 100 MB.

Cookies

We do not use any kind of cookies or other browser storage for marketing or analytics purposes, only for maintaining your login session and ensuring security. We currently use up to 4 cookies:

OAuth state token: Currently only used with single sign-on. This token is used to protect against a certain class of attacks.

Access token: Currently only used with single sign-on. This token is used for granting access to the ProcessManager backend.

ID token: This token is used to remember the identity and permissions of a user. Doubles as access token for tenants without single sign-on.

XSRF token: This token is used to protect against a certain class of attacks.

Security

To keep your data safe, we need to keep our systems secure. To do that, we have several layers of protection: HTTPS/TLS (SSL), hashed passwords and separate databases, as well as frequent updates of systems and dependencies.

For physical as well as network security of our systems, we rely on Amazon's Irish data center. Amazon's facilities are highly secure and certified for use in the payment card industry. You can read more about Amazon's approach to security here: http://aws.amazon.com/security/.

HTTPS/TLS (SSL)

TLS ensures that communication between your client and our servers is secret and have not been tampered with. To do that effectively, the server needs to be set up properly, and certificates needs to be safe. Lately, there has been lots of security with specific implementation and versions of TLS/SSL and the ciphers used, but you can be sure that your connection to our site is safe: You can use SSLLabs security scanner (https://www.ssllabs.com/ssltest/analyze.html?d=sites.process-manager.dk) to verify that our systems are not vulnerable to any of the discovered attacks on various TLS/SSL ciphers and certificates, and that our system has a secure TLS configuration.

We use HTTP Strict Transport Security to protect against certain classes of man-in-the-middle attacks.

Separate databases

The hosted ProcessManager uses a separate database per customer/domain. This minimizes the risk that your data accidentally becomes visible to other customers.

XSRF tokens

As we use cookies for our security tokens, we need to ensure that a logged-in browser cannot be tricked by another website to make requests against our service. To do that, a small token is saved as a cookie, and any request needs to include the same token in a header for the server to accept the request. As other websites cannot read the token, this ensures that these requests are coming from the ProcessManager frontend.

Data protection

We use nightly backup to Amazon's storage service, S3, to make sure your data is safe. S3 has several copies of the backups, spread out in 3 or more physically separated data centers. This ensure that even two simultaneous site-wide catastrophic accidents will not mean loss of your data. Just in case Amazon itself decides to close shop without warning, frequent backups to Google’s Cloud Storage are performed as well.