Requirements local installation

Introduction to IPscreener

IPscreener is a decision support tool based on semantic technology used for automatic prior art retrieval. When feeding a raw text to the IPscreener service, the AutoMatch search engine converts this text to a fingerprint representation. This representation is used to fetch the most similar documents reflecting the context of the query text. This is done from a specially tailored global reference database of patent documents. Thus, relevant prior art is identified and presented to a user in a client platform without any manual interaction needed. Therefore, each review of an idea along the innovation process is given a support for faster decisions, better priority of resources and at a higher quality. The tool may also be used for screening internal archives of non-patent literature such as invention disclosures, and also for classifying documents to specific company specific categories or technical domains.

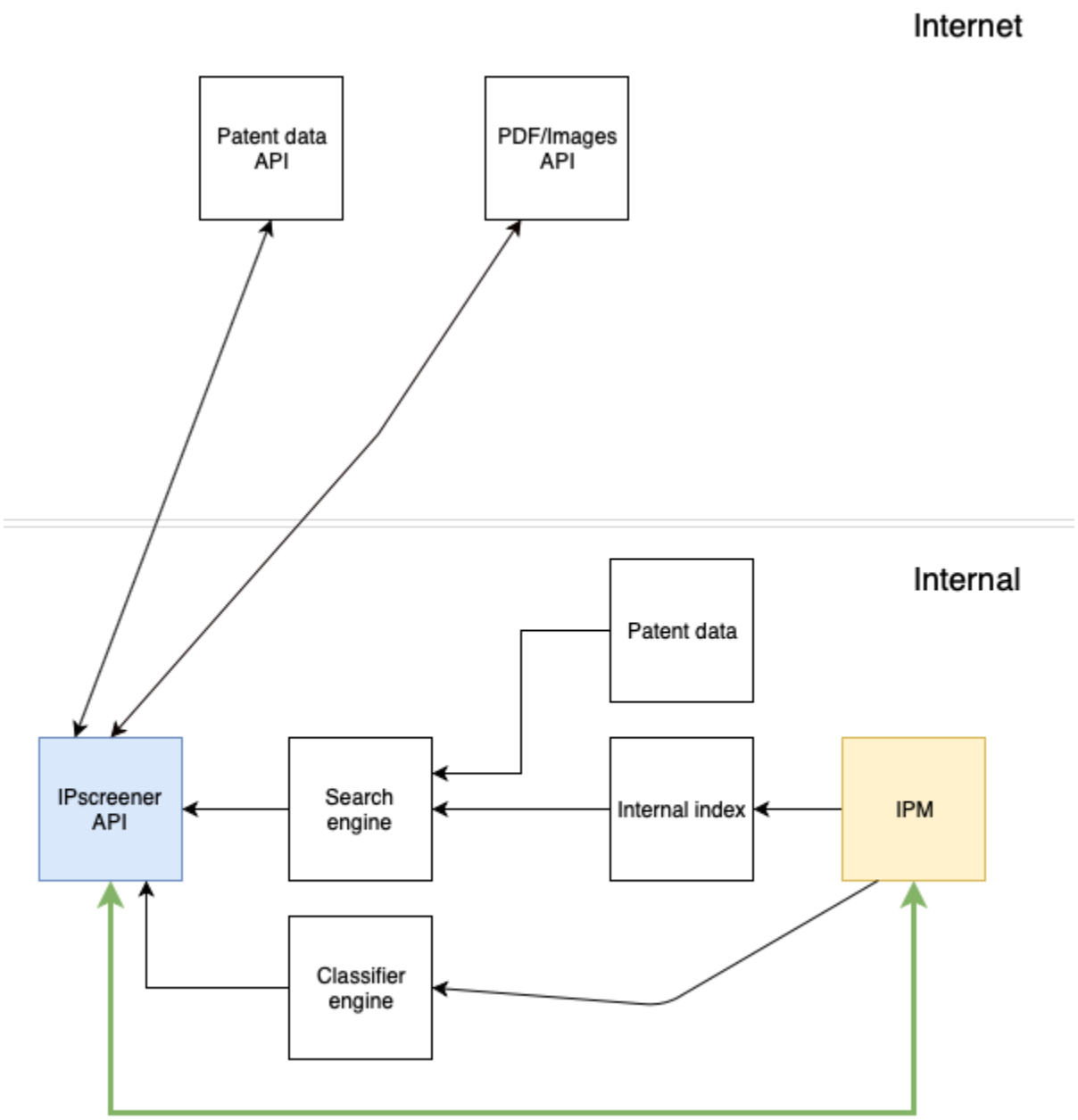
General

This is a technical documentation that describes the IPscreener Local installation and interaction with the AutoMatch search engine. The specification is intended for those who are experienced in programming software applications. This documentation is subject to continuous change, however normally backward compatibility is maintained.

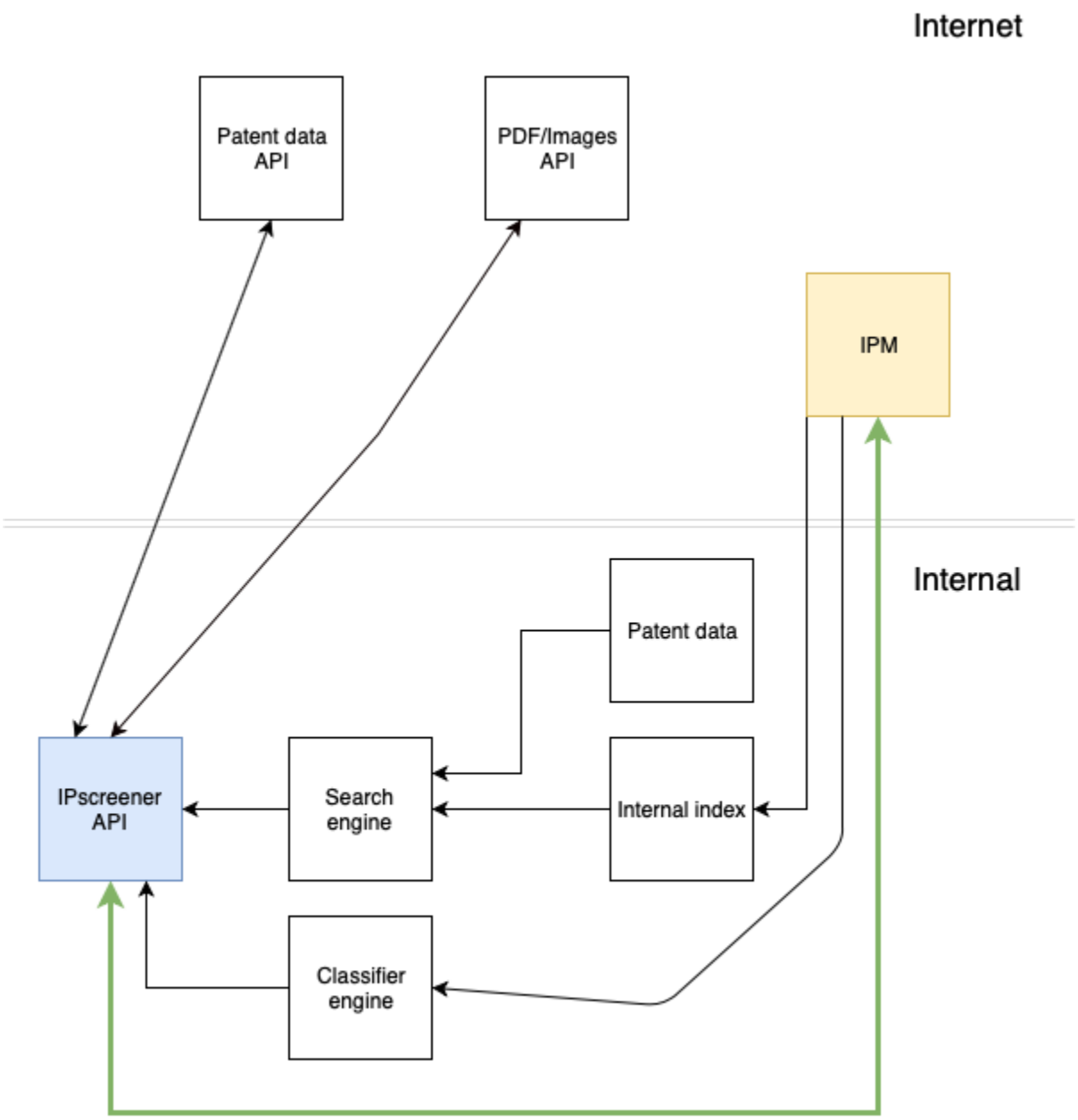
Schematic system design

The figure below shows the overall system design with communication channels for queries and data fetching. The green arrow shows the data flow for sending text query requests and for retrieving associated results. For more information on the specific query procedures and format, please consult the IPscreener API access guidelines. If IPscreener is installed locally external Internet access is only used to verify status and/or to fetch patent data, related PDF and images responding to the API outcome. If IPscreener shall screen additional prior art data from e.g. the IPM system or from the company archives (such as e.g. invention disclosures or specific non-patent related literature) a specific access loop has to be engaged. Thus, to populate the search engine and classifier engine either the client or the IPM platform push the requested data to the IPscreener platform or alternatively IPscreener is granted access to the local company/IPM APIs to fetch data for the processing procedures. No data from the IPM system is stored in raw format in our search engine or classifier, the only data stored is index-structure data. There are two general options at hand where either the IPM platform is installed locally at the client premises or hosted externally at the IPM premises, both fully compliable with the standard installation and it's functionality.

IPM system internally



IPM system externally



Minimum hardware environment required for best performance

CPU	64-bit, 4 cores
RAM	64 GB
HDD	1TB SSD
OS	Ubuntu 64-bit

The hardware backend need to provide at least 4 CPU cores with a minimum of 64 GB of dedicated RAM. We recommend to use Solid State Disks (SSD) for the installation environment, granting a minimum of 1TB of dedicated storage. This is needed for best performance of semantic AI search engine, data fetching and accessing of database indexes. Eventually local indexes of separate internal material, such as invention disclosures etc, may need additional disk storage, which is to be communicated after specific analysis. For smooth access to external patent data the IPscreener installation needs a recommended access to Internet of 1 GB/s.

Software environment required for installation

In order to perform a smooth and maximum stability of the software OS platform we recommend Ubuntu version 18 or higher (alternatively CentOS version 7 or higher). Furthermore, the installation requires Docker version 17 or higher. We recommend defining and providing associated mail server information for enabling alert, support and surveillance procedures.

Security precautions

IPscreener is provided with measurements to safeguard data and protect the software environment.

Backup

As this is a local installation we normally have no access to the internal system at the client side and empathize on the need to take daily snap shots or as frequent you wish to be able to restore data. If the client wish IPscreener to perform backup procedure we need remote access via e.g. VPN connection.

Authorization

- All communication between the client and the external IPscreener API goes through a 2048 bit encryption SSL, validated by Let's Encrypt. The web client needs to support 2048-bit SSL encryption.
- The only ports open through our firewall are 80 (HTTP), 443 (HTTPS).

Access control

There are two security layers for accessing the IPscreener service.

- SSL and the username/password, an encrypted password, never stored in plain text (combinations of different hash techniques).
- IP address range check (specific IP address or specific multi IP addresses)

Firewall and intrusion detection

hub.docker.com	TCP 80/443
***.api.ipscreener.com**	TCP 80/443

The security settings of a local IPscreener installtaion needs access to route traffic from hub.docker.com both port 80 and 443. This traffic is needed to access and download associated third party material related to patent documents and registers. Furthermore, the installation environment needs access to route traffic from the IPscreener data center domains *.api.ipscreener.com, also via both port 80 and 443. The IPscreener web server uses for communication port 80 or, if local encryption is needed, also of port 443 with your specified SSL keys provided.

Installation procedure

The setup of IPscreener needs a around 1 day for installation, setup configuration, runtime stability checks and perfomance test. We recommend an intial planning meeting disclosing the explicit installation platform review of defined performance prerequisites. Normally, we will upload the fundamental database index as pre-installation step a few days ahead due to the amount of data to transfer. Then, the final installation itself with associated validation and communication handshake verification is done remotely or on site in cooperation with the local IT team.

Terms of Use

Service Management and Support