OPSWAT - File clean-up for the TightGate file transfer

With the product MetaDefender, the company OPSWAT offers the possibility to check files with multiple virus scanners for malicious code and furthermore to remove potentially dangerous code from files (file cleaning). With file cleaning, it is possible, for example, to remove macros from Office documents without rendering the Office document as such unusable. m-privacy GmbH has recognised the possibilities of OPSWAT and offers all customers who use the OPSWAT product an interface to improve the quality of the TightGate file transfer. The following instructions describe how to configure the OPSWAT interface in TightGate-Pro.

Note

The menu items and functionality of OPSWAT are only available if the optional **opswat-integration package** has been installed.

Enabling OPSWAT changes the functionality of the TightGate file transfer so that all MIME types are automatically enabled for download, so that only the OPSWAT product decides whether a file type is allowed to be transferred. However, there is no change for the use of the file upload. This is configured as usual at TightGate-Pro and the permissions (MIME types) are assigned. The TightGate file transfer must always be used for the file upload.

Caution

Please make sure that the IP address of the OPSWAT server is not in the client network, otherwise no connection to the OPSWAT server can be established.

Menu item	Description
OPSWAT Integration*	Disables the download via the local gateway and uses only the add-on product OPSWAT for the file transfer. To configure the OPSWAT interface, the IP address of the OPSWAT server, the corresponding port and the OPSWAT rules are required. As soon as the menu item has been set to **Yes**, further menu items open below it for entering the OPSWAT details.
OPSWAT Host*	Specify the IP address or host name of the OPSWAT server. If an encrypted connection via HTTPS is used, the host name must always be entered.
OPSWAT-API-Port*	Port via which the OPSWAT server is addressed, default is 8008.
OPSWAT-Rules*	Create the rules that can be used on the OPSWAT server. The rules must correspond exactly to the name on the OPSWAT server.

Menu item	Description
Import OPSWAT-SSL-Custom-CA*	If the connection to the OPSWAT server is to be made via the encrypted HTTPS protocol, the SSL-CA of the OPSWAT server must be stored here. The CA must have been transferred to the administrator's transfer directory ***config*** in advance. If a CA has been imported and applied, an attempt is always made to communicate with the OPSWAT server via the HTTPS protocol.
Remove OPSWAT SSL Custom CA*	If a custom CA is imported, the custom CA can be removed again via this menu item.
OPSWAT client folder*	Here you can define where on the client the files cleaned or checked by the OPSWAT are transferred from the TightGate file transfer.

Note

If the user authentication is done via Active Directory, all user IDs that are to use the OPSWAT procedure must be included in the AD security group **TGopswat**. An overview of all AD security groups can be found here: Overview of AD security groups for TightGate-Pro .

Accessibility of the OPSWAT interface

If you would like to access the OPSWAT web interface from TightGate-Pro in addition to the API, the following additional settings are required:

As administrator ***config***:

- Under **Network > HTTP Out**, enter the IP address of the OPSWAT server.
- Under **Network > HTTP Ports**, enter the port via which OPSWAT can be reached. The default is port 8008.
- If you use a proxy in TightGate-Pro, the OPSWAT server must be entered as a proxy exception. This is done via the menu item **Proxy > Proxy Exceptions**. Type in the name or IP address of the OPSWAT server.
- Please do not forget to **Save** and **Apply**.

Test the setting by logging in again with a TightGate-Viewer after **applying** all settings and surfing to the OPSWAT server in Firefox. The call could look like this:

https://opswat.m-privacy.local:8008