Virus/malware scanner configuration

The file transfer from TightGate-Pro to internal clients can be monitored by a malware scanner on the server side. TightGate-Pro can be supplied with a pre-installed malware scanner as standard. Subsequent installation is also possible. In either case, a licence must be installed with which the malware scanner can be updated over the booked licence period. The licence expiry is displayed on the status page of TightGate-Pro and via the corresponding checkpoint of the Nagios system monitoring.

Note

Downloads that are downloaded from the Internet into the transfer directory of TightGate-Pro are not scanned by the virus scanner. The virus scanner is only queried when files are transferred from TightGate-Pro to the workstation.
The virus scanner is also not queried when uploading files from the workstation to TightGate-Pro.

Installing the AV scanner

TightGate-Pro can be supplied with a factory-installed and licensed malware scanner. If this is not the case, the product can be installed later if required.

How it works

- Login as administrator ***update*** and selecting the menu item **Add optional packages**.
- The following virus scanners can be installed:
  For the virus scanner from Avast, the package **avast** must be selected.
- The following is the **RSBAC-Restore** and **Apply config** in the installation dialogue.

The installation of the malware scanner starts. Once the installation is complete, please log in again as administrator ***config*** again. Under the menu item **Services** menu item, the installed malware scanner is available and can be configured.

Configuration of the AV scanner

The malware scanner is configured as an administrator ***config***.

This is required

- Installed virus scanner

How it works

- Log in as administrator ***config*** and select the desired virus scanner in the menu **Services > Malware scanner**. This opens further menu items that need to be configured.
- A free text can be entered in the menu item **Extra text**, which is displayed on the user's screen as a POP-up window if the virus scanner detects malware.

- A valid Avast license key for the product "Avast Business Antivirus for Linux" must be entered in the **License key** menu item. You will receive the key as part of the TightGate-Pro support contract from m-privacy's technical customer service.
- In the menu item **Max. number CPU cores**, you can specify how many CPU cores the virus scanner may use for scanning. The use of 4 CPU cores should be sufficient. It is recommended not to allocate more than 20% of the available cores.
- In the menu item **Max. RAM disk size in GB**, you can specify the size of the RAM disk into which TightGate-Pro automatically unpacks archives. The RAM disk is used to optimize the scan result of the virus scanner. The recommended value is 4, which corresponds to a RAM disk of 4 GB. The maximum possible input is limited to 1/3 of the total available RAM. If the value 0 is entered, no RAM disk is used.
- In the menu item **Reject encrypted archives**, you can specify whether the virus scanner generally rejects or accepts encrypted archives (e.g. password-protected ZIP files). If the value is set to **Yes**, all encrypted archives are blocked in the TightGate-Schleuse.
  Note: m-privacy GmbH generally recommends not allowing encrypted archives. In TightGate-Pro, users have the option of decrypting encrypted archives themselves before they transfer them to the internal network. To do this, they can right-click on the encrypted archive in the file manager and decrypt it.
- In the menu item **Always unpack first**, you can specify whether archives that are to be checked by the virus scanner are unpacked by TightGate-Pro before the virus scanner scans the files. This can speed up the transfer if more archives are transferred.
- In the menu item **Max. archive unpack levels**, you can specify the depth to which TightGate-Pro unpacks archives before the virus scanner gives up and blocks the file as malware. This setting is intended to prevent attacks via archive bombs. The m-privacy GmbH recommends setting a value of **5** here.
- The malware scanner can be activated or deactivated via the menu item **Malware scanner start**.
  Attention: It is advisable to check this option at the end and, if necessary, set it correctly so that the system is not inadvertently operated with the malware scanner deactivated.
- In the menu item **Malware scanner proxy**, you can set up a proxy that is used by the virus scanner to receive its signature updates. The proxy must be specified in the form IP address:port.
- Once all settings have been made, the settings needs to be saved and applied as administrator ***config*** via the menu items **Save** and **Apply**. When using the virus scanner from the company Avast, the m-privacy GmbH recommends running the Apply twice, as sometimes the required SSL CAs needs to be confirmed.
- To check whether the virus scanner is running correctly, please log in as administrator ***maint*** and call up the menu item **Malware scanner > Status**. It shows whether the virus scanner is running properly and the signatures are up to date.

Update virus signatures manually

The malware signatures are an integral part of a malware scanner. To optimise the scanner's detection performance, the signatures must always be up to date. TightGate-Pro downloads the latest definitions directly from the manufacturer's update server every day, so there is usually no need for manual intervention. If the signatures are to be updated manually, proceed as follows.

This is how it works

- Login as administrator ***maint***.

- Select the menu option **Malware scanner > Update**. The malware definitions are updated, which may take a few minutes.
- Via the status page of TightGate-Pro or the menu item **Malware Scanner > Status** menu item to check whether the signatures are up to date.

Note: In the event of an error, network problems are the most common cause. A valid licence for the malware scanner is also required.

Empty AV-Scanner cache

If a file is scanned by the virus scanner, the result of the scan is stored in the cache of TightGate-Pro for one hour. If the same file is scanned again within this time, the result of the cache is used. If files in this cache are marked as malicious code because the virus scanner was not running or had outdated signatures (> 3 days), users must wait one hour until the cache is emptied or the administrator ***maint*** clears the cache manually. The cache is emptied via the menu item **Malware scanner > Empty cache**. Please make sure that the virus scanner is running correctly and that the signatures are up-to-date before you clear the cache.

To check whether a scanner is up to date, proceed as described in the section Updating virus signatures manually.

Configure malware scanner white lists

Scanning large files (ISOs, archives etc.) by virus scanners can sometimes take quite a long time and sometimes even fail. If you have downloaded large files from TightGate-Pro and otherwise ensured that they do not contain any malicious code, it is possible to store MD5 checksums of files in TightGate-Pro for which the virus scanner does not perform a scan. The MD5 checksums can either be stored manually or already rejected files from the virus scanner log can be added to the white list.

MD5 checksum manually _ to white list __add to white list

To add an MD5 checksum to the virus scanner white list, please proceed as follows:

- Login as administrator ***maint***
- Select the menu item **Malware scanner > New in white list**
- The entry **MUST** the **MD5 checksum** followed by a freely selectable **description** followed by a freely selectable description! The file manager of the TightGate-Pro session has the following menu item in the context menu (right mouse button) **File information**from which the MD5 checksum can be copied. The MD5 checksum can of course also be determined externally. To paste a copied MD5 checksum into the selection field, use the key combination **Ctrl+Shift+v**.

Add MD5 checksum from malware scanner log to white list

To transfer MD5 checksums from an already rejected file transfer, please proceed as follows:

- Login as administrator ***maint***
- Select the menu item **Malware scanner > Rejected files**
- You will see a selection of MD5 checksums with the corresponding file names that have been blocked by the virus scanner within the last 7 days.
- Select the MD5 checksum to be included in the white list using the space bar and confirm your

selection with **OK**.
- The MD5 checksum is then accepted. It is not necessary to empty the virus scanner cache.

Remove MD5 checksum from white list

If an MD5 checksum is to be removed from the white list, proceed as follows:

- Login as administrator ***maint***
- Select the menu item **Malware scanner > Remove from white list**
- You will see an overview of all MD5 checksums stored in the white list. You can select one or more checksums using the space bar. Confirm the selection with **OK**to remove the checksums from the white list.