Integrity check (internal / external)

TightGate-Pro System integrity can be checked in order to recognise a possible compromise of the programme components or packages and initiate suitable countermeasures. A distinction is made between internal and external integrity checks.

General procedure

Each package installed in a TightGate-Pro contains MD5 and SHA256 hash values for the files it contains, which must not be changed in the system. The table with the hash values is signed by the manufacturer with GnuPG.

The integrity check runs through the list of all installed packages, first checks the signature of the MD5 hash table using the public key used for the signature and then the MD5 hash values of all files listed there. Each deviation is recorded in the log with the package and file name.

The administrator ***update*** has the separate menu option **Integrity check**, which can be used to initiate an internal integrity check during system operation. It is also possible, after starting the system from an installation medium, to select the menu option **tightgate-install > Integrity Check** menu option from an installation medium.

The difference between the check as administrator ***update*** in the running system and by the installation and rescue system prior to a so-called OE.reset is not in the algorithm, but only in where the programmes used and the public key are stored. In the case of the internal integrity check by the administrator ***update*** these are located on the hard drive of the system to be checked and could, in principle, have been manipulated, whereas when called from the rescue system or an installation disc in the run-up to an OE.reset, all programs and public keys are loaded exclusively from the read-only medium. The signed hash tables, on the other hand, are always located on the hard disc. This does not represent a security risk, as the signature check reliably excludes their manipulation.

Measures in the event of deviations during the integrity check

If the integrity check detects a change, the log file must be transferred to another system via SCP and sent to m-privacy GmbH for further investigation. The system must then be reinstalled (OE reset) to the factory settings. The configuration, the user accounts and their data must then be restored as intended. This ensures that any tampering with the files has been eliminated. If a false alarm is suspected, it is recommended that the integrity check is carried out again.

Procedure for the internal integrity check

The internal integrity check checks the installed packages of TightGate-Pro for integrity during system operation. The check is performed by the administrator ***update*** and comprises the following steps:

- Login as administrator ***update*** on the console.
- Select the menu option **Integrity check**.

The integrity check is started. Depending on system performance and the number of programme packages to be checked, the process may take some time. Using the key combination **CTRL+C** the integrity check can be interrupted. An auxiliary menu is displayed in which the check results can be displayed or transferred via SCP. It is also possible to definitively cancel the integrity check.

The result of the integrity check is summarised in a result message and saved in a detailed log file. The following values are displayed in the results message:

Value	**Description**	**Recommended action**
Correct:	Number of correctly checked packets	No action is required.
Incorrect:	Number of faulty packages	A report must be generated and sent to m-privacy GmbH .
total:	Indicates the total number of packages checked	No action is required.
skipped:	Specifies the number of skipped packages. Packages that are included as binary packages cannot be checked and are therefore skipped. These are, for example, the virus scanner or the Chrome browser.	Nothing needs to be done.
No longer installed:	Indicates the number of packages that are no longer installed as they have been deleted in the meantime.	Nothing needs to be done.

The detailed log file can be viewed using the menu option **Screen**. The following sentence should appear at the end of the screen display:

```
All analysed packages are correct!
```

Caution

If the function is cancelled prematurely, the output results report may be incorrect or incomplete.

Procedure for the external integrity check

The external integrity check checks the installed packages of TightGate-Pro against the data on an external, unchangeable data carrier. This can be a rescue system or an installation medium. The check is triggered after the system start (boot process) from the external data carrier by selecting the corresponding menu option and comprises the following steps:

- System start (boot process) from the rescue system or installation disc.
- Select the menu option **tightgate-install > Integrity Check**
- Mount the system's hard drive(s) in the directory tree: /dev/sda1 is the root partition, the rest according to the default.
- Trigger the check process.
- Evaluate the result with the menu option **Screen** or sending the test result by e-mail.

The integrity check is started. Depending on system performance and the number of programme

packages to be checked, the process may take some time. Using the key combination **CTRL+C** the integrity check can be interrupted. A help menu is displayed with which the check results can be displayed or sent by e-mail or SCP. It is also possible to definitively cancel the integrity check.

The result of the integrity check is summarised in a result message and saved in a temporary log file in the /tmp directory of the running system. Examples of result messages are

```
Positive: "All 1265 packages passed!"
```

```
Negative: "2 of 1265 packages failed. Please contact m-privacy support."
```

The number of packages to be checked may vary and depends on the actual system configuration. The temporary log file can be opened using the menu option **Screen** menu option and can only be transferred via SCP or sent by e-mail using the respective menu options, if this is provided for in the operating environment.

Caution

If the function is cancelled prematurely, the output results report may be incorrect or incomplete.