# Create backup

The configuration of the backups (data backup) is determined by the administrator ***backuser*** and the execution is also carried out via this role.

Independent of the settings for backup targets and encryption, the backup files always are additionally saved locally on the TightGate-Pro in the directory **/home/backuser/backup** of the administrator ***backuser*** unencrypted. They remain there until they are either manually deleted or the expiry date is reached.

USB mass storage devices or backup servers located in the network can be selected as additional storage locations. In addition to the time-controlled call, the creation of backups can also be triggered manually via the menu item **Backup**, whereby the settings made in the configuration menu are applied.

#### Hinweis

If backups are to be transferred manually, please note the information in the FAQ on TightGate-ProHow can I transfer backups manually?

## Creating local backups

Here's how

- Log in as administrator ***backuser*** and call the menu item **configuration**. The following configuration options are also available:

| Menu item | Description |
|---|---|
| Lifetime | The lifetime of a backup is specified as an integer between 0 and 60. It describes after how many days the files are automatically deleted from the local directory **/home/backuser/backup** of the TightGate-Pro server. Here, 0 means that every previously stored backup is deleted. This mechanism only applies to local backups on TightGate-Pro. If backups are stored on external servers or storage media, other measures must be taken to delete obsolete data. |
| Frequency | For the time-controlled creation of data backups, you can set whether the cycle should be **Daily**, **Weekly**, **Monthly** (at 4 a.m. each day) or **Individual**. Within the scope of the individual settings, the day of the week, hour and minute (5min window) can be precisely determined, whereby more than one selection is possible. |
| Backup type | The backup type decisively determines which data can be restored later. To facilitate the selection, see the following Overview. |
| Backup Extra Name | A specific name for this TightGate-Pro (node) can be used here. Adding the specific name changes the naming of the backup for this server from **back-date** to **back-extraname-date**. |
| Import SSH key | Import the SSH key for the backup server to be able to upload backups via SCP or SFTP.<br>Please note that the key must first be stored in the "Keys" directory of the administrator ***backuser*** . |

**Hinweis**

Log files are created for subsequent analysis of automatic backup runs. These can be viewed via the menu item **Show last log**. No log is created for manually triggered backup runs.

# Backup to backup server

In addition to the local backup on TightGate-Pro, it is recommended to store an additional backup on a remote server or a USB storage medium.

This is required

- IP address of the backup server
- Access data and directory of the backup server
- SSH key for encrypted transmission, if applicable.

This is how it works

- Log in as administrator ***config*** and call up the menu item **Services > Backup server.**
- Add the backup server(s) under **New entry** (resolvable computer names or the IPv4 addresses) or edit or delete existing servers under **Backup server**
  **Note:** If the backup is to be written to an FTP server located in the client network area, the backup server must also be entered in the list of permitted FTP servers under the menu item **FTP outgoing**.
- Settings **Save** and **Apply**
- Log off as ***config*** and log on as ***backuser***
- Call the menu item **configuration**
- As **upload procedure SCP** or **SFTP** are available. After selecting an upload method, a submenu appears with the respective configuration options:
- Under the menu item **Server**, a backup server (created as ***config*** ) can be selected.
- Under the menu item **User** the user name for the backup server is to be entered.
- Under the menu item **Remote directory**, enter the complete path of the target directory.
- Please save the settings **afterwards**
- To avoid being asked for the password for the user on the target server with every backup, an SSH key can be used for the user. This can either be created on TightGate-Pro and then imported into the backup server or an existing SSH key can be copied into the transfer directory of ***config*** and then imported as ***backuser*** .

Recommendations from m-privacy GmbH

- After each reconfiguration of the backup settings, a backup should be created manually to test the settings.
- It is generally recommended that backups are not only kept locally on the TightGate-Pro, but that copies are stored separately.
- Here you will find instructions on how to save a backup on a Windows server –> Instructions

# Backup to USB memory

To save a backup to a USB hard disk, some preliminary work is necessary. First, a label name must be assigned for the USB hard disk.

If several hard disks are used, they must all be given the same label name. Each USB hard disk must be formatted with the ext (extended) file system for use with TightGate-Pro Server. Since this is a Linux-based file format, the following instructions for preparing the hard disks refer to a Linux distribution. After preparing the hard disks (see below), set up TightGate-Pro Server.

The following steps require logging in as ***backuser*** . In the menu **configuration** the following operations are to be carried out:

- Menu item **Backup part. label:** Enter the label name, i.e. the name of the external hard disk.
- Menu item **Backup-Part.-TTL:** Entry of the retention time of the backup files on the USB hard disk.
- Menu item **Save:** Backup of the settings.
- Connection of the USB hard disk with TightGate-Pro Server.
- Menu item **Backup:** Manual start of data backup.

It is recommended to check the correct data backup on the USB hard disk manually.

For hard disk preparation under Linux, ***root*** -rights are required. The following steps are carried out on the console.

To perform the following actions and commands, you need administrator access (root rights). For the following actions, please open a console.

**Partitioning the USB hard disk**

Please create a partition that is of the type Linux:

```
fdisk /dev/sdb*
```

*please specify the exact drive name (usually sdb). Then perform the following actions:
- p (display the current partition table)
- d (delete the partition)
- n (create the partitions)
- w (write the table and quit fdisk)

**Formatting and Partitioning the USB Hard Drive**

To format the hard disk, enter the following command:

```
mke2fs -j -L TG-Backup /dev/sdb1*
```

*please specify the exact partition (usually sdb1)

**ATTENTION:** In case several hard disks are used, they must all have the same label name!

**Switch off hard disk check**

Please switch off the hard disk check for the USB hard disk with the following command:

```
tune2fs -i 0 /dev/sdb*.
```

*please enter the exact drive name (usually sdb)

# Encryption of the backup

To protect data backups on external media from unauthorised access, we recommend encrypting the backups with GnuPG.

This is how it works

- Create a GnuPG key pair on your own (see http://www.gnupg.org/)
- Copy the public GnuPG key via SCP into the directory **~/keys** of the administrator ***backuser***
- Select the key to be used in the backup configuration under the menu item **New GnuPG key**

Hint:

- Create a new connection definition for WinSCP. Select **SCP** as the protocol.
- Under the menu item **Advanced > SCP/Shell** enter the following in the menu item **Shell**: **/bin/loginbash**
- Under the menu item **Advanced > Directory > remote directory** enter the following: **/home/backuser/keys**

# Overview of backup scope

For the individual backup types, a new complete backup with different scope is written in each case. The following table describes the scope of the respective backup types:

| Type / scope | System configuration | Bookmark archive | User IDs | User profiles | User profiles (optimised) | Transfer directories |
|---|---|---|---|---|---|---|
| System only | X | – | – | – | – | – |
| System, bookmark archive | X | X | – | – | – | – |
| System, user, bookmarks | X | X | X | – | – | – |
| System, user, no transfer | X | X | X | X | – | – |
| System and user data | X | X | X | X | X | X |
| System, ben., opt., no transfer | X | X | X | – | X | – |
| System, user data optimised | X | X | X | – | X | X |

Basically, the backup does not include:

- Program and system files that are part of the installation packages for TightGate-Pro and
- installation files and configuration data of add-ons for the web browser installed by the user.

**Legend:**

System configuration
Backup of system configuration (network connections, proxy etc.) to restore TightGate-Pro. No user IDs or profiles are backed up.

Bookmark archive
Backup of the bookmark archive to restore bookmarks for individual user IDs.

**Hinweis**

In order for the bookmark archive to be saved in the backup, the administrator ***config*** must be switched on under **System Preferences > Bookmark Archive = Yes** and the number of days a bookmark is to be kept in the archive must be specified under **System Preferences > LZ Archive Lifetime**.

User IDs
Backup of user IDs, including user attributes such as (transfer authorisation, audio, clipboard etc.) as well as login data (passwords, certificates etc.).

User profiles
Backup of the complete user profiles.

User profiles (optimised)
Backup of an optimised version of the user profiles, which only contains the usual data to be able to restore a user from a backup.

Transfer directories
Backup of the complete transfer directories of all users.