Create backup

The configuration and creation of backups (data backups) is carried out by the administrator ***backuser***. Regardless of the settings for backup destinations and encryption, backup files are also created **locally on the TightGate-Pro** in the directory **/home/backuser/backup** directory without encryption. The files remain there until they are either deleted manually or the configured expiry date is reached.

In addition **USB mass storage devices** or **backup servers in the network** can be used as storage locations. Backups can be both **time-controlled automatically** as well as **manually** be created. The settings defined in the configuration menu are used for the manual start.

Hinweis

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

As a rule, backups are created automatically according to a schedule. The corresponding settings are described in the following sections.

Backup configuration

The following settings must be configured, regardless of whether backups are only saved locally or are also transferred to an external medium or a backup server. The configuration is carried out via the menu item **Configuration**.

Menu item	Description
Time To Live	Specifies after how many days backups are automatically deleted. Permissible value range: **0-60 days**. The value **0** means that every previously stored backup is deleted. This mechanism only applies to local backups on the TightGate-Pro. The deletion of obsolete data must be organised separately for external storage locations.
Frequency	Defines the schedule for the automatic creation of backups. Possible options: **Daily**, **Weekly**, **Monthly** (each at 04:00 a.m.) or **Individually**. With customised settings, you can **day of the week, hour and minute** (5-minute grid) can be freely selected. Multiple selections are possible.
Transfer backup	Determines whether the **transfer directory of the user** is included in the backup. For reasons of backup size, it is recommended that this option **not to activate this option**.
Shared Folder backup	Determines whether the shared directory **tgshare** is included in the backup. Here too, it is recommended that this option **not to activate this option**to keep the backup size small.
Backup Extra Name	Allows you to assign an additional name for this TightGate-Pro. This changes the naming of the backup files from **back-date** to **back-extra-name-date**.

Menu item	Description
Import SSH pubkey	Import an SSH key for the backup server in order to create backups via **SCP** or **SFTP** to be able to transfer backups via SCP or SFTP. The key must first be stored in the **keys** directory of the administrator ***backuser*** directory beforehand.

After completing the configuration, the settings must be saved via the menu item **Save** menu item.

You can then save the settings via **Main menu > Backup** to create a backup.

Hinweis

For traceability, a backup log is created for each backup. **backup log** is created for each backup. This can be viewed via the menu item **Show Last Log** menu item.

If the backup is also to be transferred to an external medium or a backup server, the corresponding settings must be made in accordance with the following sections.

Backup to backup server

Backup to external backup server

The backup of backups on an external backup server is configured as follows.

Prerequisites

The following information is required:

- IP address or host name of the backup server
- Access data for the backup server
- Target directory on the backup server
- Optional: **SSH key** for encrypted transmission

How to proceed

- Login as administrator ***config***.
- Call up the menu item **Services > Backup Server**.
- Under **New entry** add a backup server (host name or IPv4 address).
- Settings **Save** and **Apply**.
- Logout as ***config*** and login as ***backuser***.
- Call up the menu item **Configuration**.
- Select the upload method **SCP** or **SFTP**.

Additional configuration options appear after the selection:

- **Server** - Selection of a server previously configured as ***config*** backup server
- **User** - User name for access to the backup server
- **Remote directory** - Complete path to the target directory

- **(Re)set SSH key** - generated when **saving** a new SSH key when saving the configuration
- **View the SSH public key** - Displays the current SSH key on the screen
- **Upload the SSH public key** - Attempts to upload the SSH key to the external backup server

- After configuration, the settings can still be saved via the menu item **Save** menu item.

Hinweis

Here you will find instructions on how to save a backup to a Windows server –> instructions

Backup to USB memory

Some preliminary work is required to save a backup to a USB hard drive. Firstly, a label name must be assigned to the USB hard drive.

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

The following steps require the login as ***backuser*** is required. In the menu **Configuration** menu, the following operations must be carried out:

- **Backup Disk Label:** Entry of the label name, i.e. the name of the external hard drive.
- **Backup Disk TTL:** Entry of the retention time of the backup files on the USB hard drive.
- Afterwards save the settings via **Save**.
- Connection of the USB hard drive to TightGate-Pro Server.
- Menu item **Backup:** Manual start of the data backup.

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

The hard drive preparation must be carried out on another Linux system, not on the TGPro server itself. Under Linux, this requires ***root***-rights are required. The following steps are carried out on the console.

To be able to carry out the following actions and commands, you need administrator access (root rights). Please open a console for the following activities.

Partitioning the USB hard drive

Please create a partition that is of the Linux type:

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

*Please enter the exact drive name (usually sdb) Then carry out the following actions:
- p (display the current partition table)
- d (delete the partition)
- n (create the partitions)
- w (write the table and exit fdisk)

Formatting and partitioning the USB hard drive

To format the hard drive, please enter the following command:

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

*Please enter the exact partition (usually sdb1)

CAUTION: In the event that several hard drives 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 designation (usually sdb)

Optional: Encryption of the backup

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

How to proceed

- Independent generation of a GnuPG key pair (see http://www.gnupg.org/)
- Copy the public GnuPG key via SCP into the directory **~/keys** directory of the administrator ***backuser***
- In the backup configuration under the menu item **New GnuPG key** select the key to be used

Note for WinSCP

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

Overview of backup scope

TightGate-Pro creates a standardised backup that contains all the data required to restore users or as part of a **disaster recovery scenario** set up a new TightGate-Pro system as part of a disaster recovery scenario.

Included components

- System configuration (all configuration settings)

- Bookmark archive (browser bookmarks and saved passwords)
- User IDs (login data and authorisations)
- User data from additional packages, e.g. **beBPO**

Optionally included

- Transfer directories of the users
- System-wide shared folder **tgshare**

Not included

- Programme and system files that are part of the installation packages from TightGate-Pro
- Installed optional extension packages
- Installation files and configuration data of browser add-ons installed by the user