

Installation for Advanced Data Protection and Standard Installation

GDPR (<https://www.eugdpr.org/>) is a European Union (EU) directive, which replaced the Data Protection Directive 95/46/EC on May 25, 2018. The objective is to harmonize European data protection laws while focusing on strengthening EU citizens' rights protecting their personal data. All companies and organizations, which process EU citizens' data, are affected, regardless of where these companies or organizations are based and where the data are being processed. Particularly in the healthcare sector, this implies that every person dealing with personal (patient) data must adhere to the GDPR. In addition to hospitals, medical practices, pharmacies, laboratories and health insurances (to name but a few), manufacturers of medical technology products are equally affected.

Sentec therefore revised V-STATS including V-CareNeT in order for the user to adhere to GDPR. Each individual organization (hospital, medical practice) may determine whether they save patient data and which data should be saved. The organization is responsible for complying with applicable regulations. With this release, Sentec offers measures which allow GDPR-conform handling of patient data.

Starting with Version 5.00, V-STATS may be installed as Standard Installation or Installation for Advanced Data Protection. The following table provides an overview of the main differences between these two installations. All the other main functions of V-STATS/V-CareNeT (Downloading/ Importing SDM Trend Data, Administration of Profiles, etc.) not listed in this table are available in both installations.

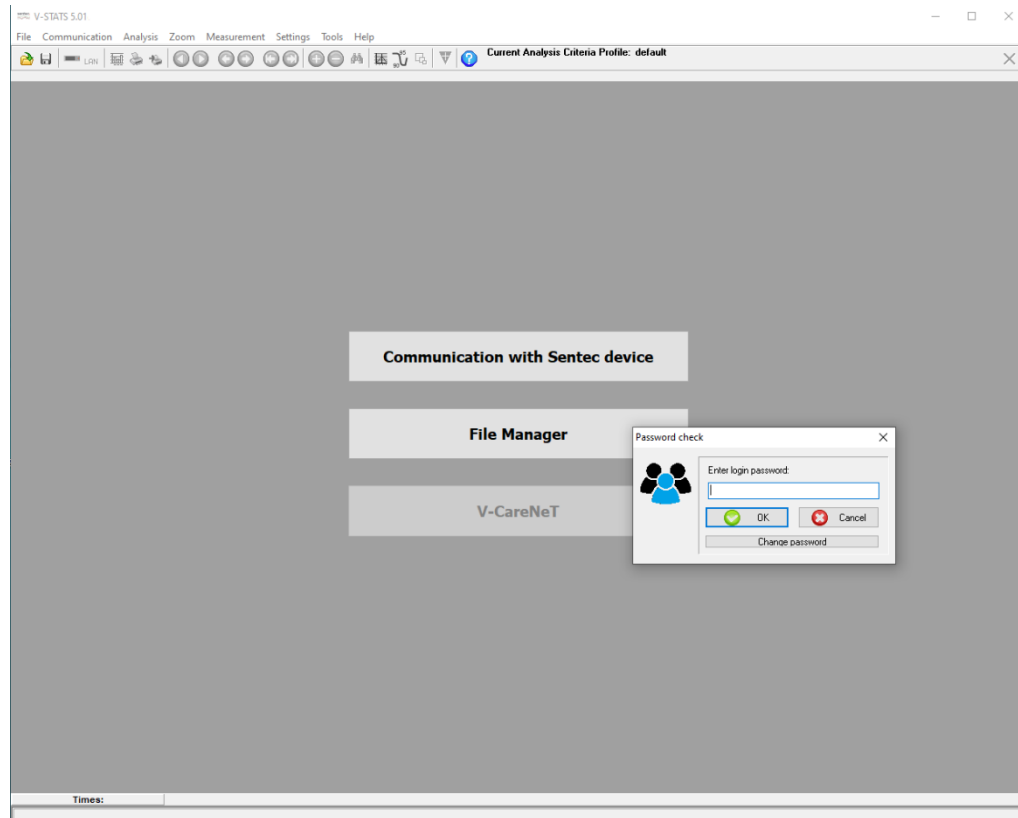
V-STATS/V-CareNeT Installation and functionality	Standard Installation	Installation for Advanced Data Protection
Additional features to support fulfilment of GDPR (General Data Protection Regulation) requirements	–	✓
Login Password	–	✓
Admin Password allows access to: <ul style="list-style-type: none"> • V-STATS Settings • SDM Profiles • SDM Configuration Special Functions	✓	✓
Encryption of patient data	–	✓
Handling of encryption keys	–	✓
Restoring forgotten passwords	✓	–

***Note:** Check with your local IT department whether you need to use the Installation for Advanced Data Protection. The organization is responsible for complying with applicable regulations.*

The following points provide an overview of the GDPR (General Data Protection Regulation) requirements, indicate where V-STATS/V-CareNeT are affected and how these requirements are met with installing the Installation for Advanced Data Protection in particular.

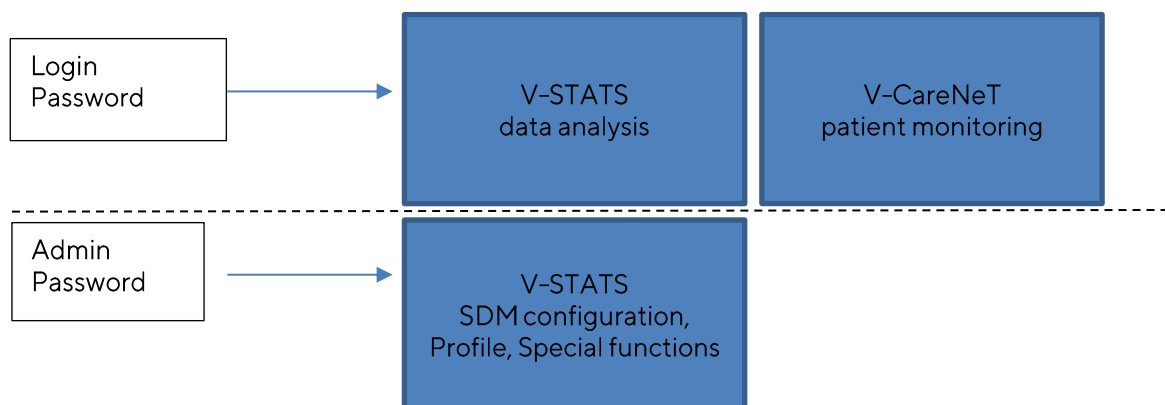
- A) Preventing unauthorized access of patient data, protection of unauthorized use of the infrastructure needed for patient data processing.

V-STATS' Installation for Advanced Data Protection has a login function. A login window appears upon starting the program where the user must enter a password in order to be identified as a legitimate user. Thus, unauthorized persons may not access V-STATS. Authorized users may only view data which they are permitted to view.



The password for protecting V-STATS Settings, SDM Profiles & Configuration and Special Functions is referred to as Admin password in order to differentiate it from the Login password.

***Note:** Using V-CareNeT (licensed version) does not require a separate login.*



- B) Unauthorized access of data must be prevented. If necessary, supervisory authorities and the data owner (patient) must be informed. The encryption of patient data is a measure for preventing unauthorized access. This encryption is a sufficient measure for preventing infringement of protection.

For this reason, Sentec implemented patient data encryption with the AES256 encryption algorithm. In order to encrypt patient data, a key needs to be created upon Installation for Advanced Data Protection if the previous version is lower than version 4.10. Key creation happens at a click of a button as V-STATS has a dedicated function for doing so. Subsequently, V-STATS will use this key automatically; a copy must be stored safely and may be exported if necessary (e.g. to hand over patient data to another authorized person).

- C) Upon installation, existing unencrypted data are being not encrypted automatically with the new key.

Upon **Update** from V-STATS version lower than version 4.10, unencrypted data in the target folder as well as sub-

directories are also not encrypted automatically. Users may do this manually at a later stage. After first start-up of V-STATS a dialog pops up if unencrypted data exist in the target folder. The user may then select whether unencrypted data shall be encrypted.

Encrypted data that have been encrypted with a key from V-STATS version 4.10 remain readable / changeable upon Installation for Advanced Data Protection. During update the User is not asked to generate a new key or to load an existing key if a key is already available from previous version 4.10.

- D) It is still possible to enter patient data. However, before entering data the user must check the box "Activate personal data" and confirm the subsequent data protection warning. This applies to both, V-STATS and V-CareNeT.

When downloading data (from an SDM), these data are automatically encrypted. Measurement values and patient data are saved separately, whereby the patient data are encrypted.

Note: Should you require support from Sentec, never send any patient data to Sentec or your local Sentec representative.

- E) Patients have the right to receive their data in a common, machine-readable format. The already present data export within V-STATS fulfils this requirement, for example even converting and exporting in the EDF+ format.