October 9, 2002

DATATRACE® for Windows
Password Protection, Electronic Signature, and Audit Trail Capabilities

Introduction

The DATATRACE system allows you to collect process time and temperature, humidity, or pressure data with minimal disruption because these unique dataloggers (Tracers) can be placed directly into the target application. The DATATRACE® for Windows (DTW) software provides the interface for your computer to program and read Tracers. Then the program can be used to analyze and manage the data collected. The DATATRACE system provides this vital information without depending upon external connections; the Tracers are completely self-contained sensors.

Accurate knowledge of processing parameters give you increased confidence that your products and processes satisfy your operational requirements and meet any appropriate regulatory requirements. DTW can also provide enhanced data and program security to meet regulatory guidelines, if necessary.

Security Information On DATATRACE® for Windows

This version of DATATRACE® for Windows was developed with a sophisticated security system to protect data and to comply with US Food and Drug Administration's regulation 21 CFR Part 11.

For those users who are not required or interested in this level of security and the operational complexities that go along with it, DTW can be installed without any additional security elements. However, as in past versions, DATATRACE® for Windows provides a sophisticated verification of data integrity each and every time you collect and retrieve data. This level is adequate and appropriate for most users of the DATATRACE system.

DO NOT USE A SECURITY LEVEL THAT IS NOT REQUIRED BY GOVERNMENT REGULATION OR CORPORATE REQUIREMENTS!

If you do not wish to install DTW with enhanced security, when the Security window appears at the end of the installation procedure, make sure that "No" is selected and click OK to complete the installation of DATATRACE for Windows without enhanced security.

Should you need enhanced security levels, or if you are just curious, read on.

There are two levels of enhanced security available for DTW: "User" and "Full". These options are identified on the Security window that appears near the end of the DTW installation procedure. In both cases, the Administrator of the system should make the initial installation of the DTW program. The Administrator assigns passwords and authorization levels and is responsible for system security.

As with all effective security systems, if you forget your password not even your system administrator can help you.

Installing DATATRACE® for Windows With Security

DATATRACE® for Windows includes an automatic installation program that is initiated when the DATATRACE CD is inserted in the CD-ROM drive. When the Installation Wizard starts, just follow the instructions that appear on the screen.

When completed the program updates the System Configuration for the DATATRACE® for Windows program and displays a document on Security. DTW security capabilities include password protection and data encryption. When enhanced security levels are enabled, access to various program functions can be strictly controlled. In addition, the program can enable capabilities for compliance with US FDA's 21 CFR Part 11.

DTW will require, during the installation process, you define the level of security you wish to operate the program under. The options are **No Security**, **User Security**, or **Full Security**. The level of protection defined during program installation can not be modified when the installation process is complete.

> **No Security** allows the user or users to access all functions of the program without restriction. It bypasses most of the cryptographic features of the program. The only cryptography employed in this case is the addition of SHA-1 algorithm for data profile security. Most users will find this is appropriate for their activities and does not require additional procedures for the user.
>
> **User Security**, in addition to the SHA-1 algorithm, requires that the user login with a User ID and Password in order to access the program. Each user is also assigned one of three possible authorization levels: "Data Only", "Data and Utilities", or "Administrator". These authorization levels allow access only to those function levels of the program that the user has been approved for. User Security **does not** implement data signing or auditing necessary to meet US FDA's 21 CFR Part 11.
>
> **Full Security** complies with US FDA's 21 CFR Part 11 and, in addition to the password protection provided with User Security, Full Security provides for "Electronic Signatures" and an audit trail of user activities within the program.

Make your selection and click OK.

A new screen appears when the installation is complete. Press Finish and then close the Internet Explorer and the display returns to your Desktop. Note that a shortcut was installed on your desktop for the DATATRACE® for Windows program.

STORE THE ORIGINAL DATATRACE® for Windows CD IN A SAFE LOCATION.

The following provides an overview of the procedures for enabling the secure levels of program operation.

Data Validation and Encryption

With the DATATRACE® for Windows program, each Tracer you Read has a validation code calculated and stored with the profile data before any other operation is performed. The validation procedure occurs with all security levels. The validation code can then be checked whenever the profile is accessed to verify if the profile has been corrupted or changed in any way.

You can not disable the data validation process. Whenever the profile is output or displayed the validation status of that profile is reported.

There are three status values reported:

The first reports the status “As Collected”. This indicates that the profile has not been changed.

The second reports the status “Modified” when the values indicate the profile has been changed.

The third reports the status “Disabled” when the profile was generated from old DOS files (RPT, DPT, DPP, or DPH) imported into the DATATRACE® for Windows program.

There are several encryption routines used in the DATATRACE® for Windows program for security purposes. Some are used regardless of security mode on the collected data and stored with the profile data, while others are used for the security system itself (e.g., passwords, private keys, etc.).

User Security

During installation the user selects the level of security that the DATATRACE® for Windows will function under. If “User” or “Full” security is to be enabled, the individual that is assigned the “Administrator” role should be involved in, and responsible for, the installation of the DTW program.

Immediately after installation in both enhanced security modes, the program will request a Login and Password. The Administrator enters “admin” (without quotation marks) in both text boxes. Be aware, this combination will only work the first time it is used.

After you enter “admin”, “admin” a dialog box will appear and require that you change to a new Password. This is not negotiable! You must change your password to include at least 8 characters and at least one of them must be numeric, no spaces. When the program is instructed to save the new password, there will be a delay while the new password is recorded, encrypted, registered, and stored.

Don’t Forget Your Password! This is now the only password that will work at the Administrator level of password protection. This is important because the Administrator is the only one that has access to the SETUP tab and assigns the authorization levels for other users.

The SETUP tab available to the Administrator includes all of the functions from previous DTW versions plus a new one: a USERS Tab. The USERS Tab establishes, lists, and defines all authorized users when either of the enhanced security modes is selected during installation of the DTW program. This data is only accessible by the program Administrator in order to maintain the security of the system.

Adding New Users

DATATRACE® for Windows has security capabilities that include password protection. When enabled, access to various program functions can be strictly controlled through various password authorization levels. In either of the enhanced security levels, it is imperative the user remember their User ID and Password. There is no salvation for a lost password. This is a requirement for the various security systems. The following provides an overview of the procedures for establishing new user passwords:

The USERS Tab allows the administrator to establish new users. This function is only accessible by the administrator. The administrator adds a user by clicking the Add User button under the USERS tab. A dialog box appears asking for New User data: a Login ID, the users full name, and his security level. When the Save button is pressed the new user is added to the Users List. The new user is active and has access to his/her authorized levels when there is a check mark in the Active check box of their User data.

It is important to note that a user can not be removed from the Users List, only deactivated. Deactivation is accomplished by removing the check mark from the Active check box. When inactive, this user can not access the DTW program.

The first time a new user tries to enter into the DTW program, they are asked for the login information that was created by the Administrator. On this first access to the program, and only on the first access, the new user enters the Login ID entry provided by the Administrator for both the User ID and Password. A dialog box will appear and require that the new user change to a new password. This is not negotiable! The new user must change his/her password as instructed on the dialog box: at least 8 characters and at least one of them must be numeric, no spaces. There will be a delay during the save.

A non-administrator user has only two options for authorization levels: “Data Only” or “Data and Utilities”. The Administrator assigns these authorization levels. No one has access to the Setup options except the Administrator.

Full Security

While the User mode discussion above defines the Password security that is enabled for both “User Security” and “Full Security”, it does not address the additional capabilities of the “Full Security” mode. These include “Signing” and “Audit” capabilities as required by the USFDA 21 CFR Part 11. Attached to this document is a listing of the 21 CFR Part 11 requirements for a “Closed System” and a summary of DATATRACE® for Windows’ compliance. Note that not all 21 CFR Part 11elements applies to DTW. A **Closed System** is defined as “…an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.”

Data Signing occurs only in “Full Security” mode. Data Signing in DATATRACE® for Windows requires Tracer reads to be digitally “signed” by the user. When a Read is attempted, the user is prompted for his/her User ID and Password. The program then locates and verifies the user record in precisely the same manner as a login, then further verifies that the login information matches the user that is currently logged in to the system. If successful, the user’s private “signing key” is affixed to the profile along with the User ID.

”Signing Keys” are electronic pairs of encrypted codes that uniquely define that a user is who they say they are. These keys are a matched pair: one “public” and the other “private”. By comparing and verifying the user’s “private” key, DTW in “Full Security” mode verifies the “Signature” of the user for the target profile. Upon retrieval, the profile exhibits the user’s “public” key on the profile.

System Auditing occurs only in “Full Security” mode. This function generates and maintains an audit trail for certain system events and user activities and stores them in a secure, encrypted table. This table includes: User ID, a date/time stamp, and an action description.

Logging an Audit Trail

In the “Full Security” mode of the DATATRACE® for Windows program certain functions that a user performs in the program are logged in the Audit Trail. For each logged event the User ID, the date/time the action occurred, a description of the action, and a hidden, encrypted code to deter tampering are stored.

The following actions are automatically logged in the Audit Trail table when in Full Security mode:

User Login

User Exit

Add/Edit of User Record

Tracer Program (description contains Serial Number, Run ID, and Start Time).

Tracer Read (description contains Serial Number and Run ID).

rH Tracer Calibration (description contains Serial Number and Calibration Type).

Profile Export (description contains Serial Number, Run ID, and Start Time).

Data Archive (description contains Serial Number and Run ID).

The Audit Log can be printed for review or security auditing.

As indicated earlier it is important to use the security capabilities appropriate to your needs. In general, do not use a security level that is not required by government regulation or corporate requirements.