



VICTORINOX

# Presentation Master Victorinox Secure USER'S GUIDE

Version 1.0.1





# USER'S GUIDE





Foreword .....	7
Compatibility .....	9
Important Issues First .....	10
Getting Started.....	11
Fingerprint Recognition.....	12
Login Screen.....	20
The Caption and the Navigation Bar .....	21
Internet Features .....	22
Sync Favorites .....	22
Safe Browsing .....	24
Outlook Menus .....	25
Outlook Express .....	25
Backup to USB Stick.....	26
Restoring and Managing Backups.....	27
Microsoft Outlook .....	28
Create & Synchronize.....	28
Overwriting Outlook Information.....	31
Delete Outlook Profiles .....	32
Synchronizing.....	33
Your Documents.....	34
Folder Synchronization.....	35




---

Settings	37
Synchronization Settings.....	37
Security Settings.....	38
Windows Login using A Fingerprint.....	40
Device Information .....	44
Encrypted Drives.....	45
Creating a Drive .....	45
Starting a Drive .....	49
Closing a Drive .....	50
Deleting a Drive .....	51
Managing Fingerprints .....	52
The Password Manager .....	53
Adding a Password.....	54
Changing a Password .....	56
Deleting a Password.....	57
The Bluetooth Module .....	58
Connecting the Bluetooth Module .....	58
Working with the Bluetooth Module.....	60
Bluetooth Problems and their Causes.....	61
Support Information .....	62
Notes and Legal Issues.....	63





## FOREWORD



We would like to congratulate you on the purchase of your new, high quality Victorinox pocket tool. In the development of the Presentation Master / Victorinox Secure, particular attention was paid to making its usage as simple and intuitive as possible. Through the addition of a fingerprint

reader, a new standard of security has been achieved: While passwords can be guessed and shared, it is not possible to do that with fingerprints.

We would like you to know that you can only be authenticated by a registered, uninjured finger.

This guide describes the use of the Victorinox Presentation Master and Victorinox Secure products. Their equipment differs as follows:

- |                             |   |
|-----------------------------|---|
| Presentation Master:        | <ul style="list-style-type: none"><li>- Laser pointer</li><li>- Bluetooth Remote Control</li><li>- Biometric USB 2 Stick</li><li>- Blades</li></ul> |
| Presentation Master Flight: | <ul style="list-style-type: none"><li>- Laser pointer</li><li>- Bluetooth Remote Control</li><li>- Biometric USB 2 Stick</li></ul>                  |
| Victorinox Secure:          | <ul style="list-style-type: none"><li>- High performance LED</li><li>- Biometric USB 2 Stick</li><li>- Blades</li><li>- Ball Point Pen</li></ul>    |
| Victorinox Secure Flight:   | <ul style="list-style-type: none"><li>- High performance LED</li><li>- Biometric USB 2 Stick</li><li>- Ball Point Pen</li></ul>                     |



All of these products are supplied with a special USB 2 extension cable. Although the biometric USB stick can be connected directly to a USB port on a notebook, we recommend always using this cable. Doing so allows the fingerprint reader to be operated while it is in a flat position on a table. Notebook ports are not intended to absorb the mechanical forces which might arise from using the fingerprint module while it is connected directly to a notebook.

**CAUTION: Please use the supplied extension cable exclusively in connection with the biometric USB 2 module. The cable is not for use USB devices other than your biometric USB module.**

Regarding the laser pointer, high-power LED, blades and ballpoint pen features, please read the individual guides printed and provided with your purchase. You will also find the guarantee provisions and guide to changing batteries in those guides.

The USB stick was formatted using exFAT (Extended File Allocation Table) at the factory. The exFAT file system was specially developed for flash memory. Above all, the advantages include a maximum file size of 16 Exabytes and the introduction of a table that indexes the free clusters. Owners of Windows Vista may receive exFAT by installing Service Pack 1. ExFAT support is available as an update for Windows XP in Service Packs 2 and 3 and may already be present (depending upon your automatic update settings). These updates will however request that you format your new Victorinox Presentation Master or Victorinox Secure products when you first connect them to your computer.

You can find the exFAT update for Windows XP (KB955704) at:

<http://www.microsoft.com/downloads/details.aspx?familyid=1CBE3906-DDD1-4CA2-B727-C2DFF5E30F61&displaylang=en>





## COMPATIBILITY

In order to be able to use all of the features of this product, you will need a computer with the following characteristics:

- Intel or AMD Processor
- A free USB 2 or USB 3 port
- Windows XP SP 3 (Service Pack 3),  
Windows Vista 32 / 64 Bit SP 1  
or Windows 7 32 / 64 Bit
- MS Internet Explorer 7 or later, or Firefox (if you would like to use the Internet features)
- MS Outlook 2007 or later, or MS Outlook Express (if you would like to use the Outlook features)

You will also need extensive rights on your computer, such as the right to start an application and the rights to register and use a USB device. In order to be able to use all of the features, you will need local Administrator rights.

For the usage of the Bluetooth module (only with the Presentation Master and Presentation Master Flight models), your computer will also require a Class 1 or Class 2 Bluetooth receiver with an installed Bluetooth stack compatible with the Microsoft standard.

**CAUTION:** If problems arise when using the software or registering the Bluetooth module, please contact your System Administrator or local support team first. These specialists will be able to ensure that you have sufficient rights on your computer for using this product.



## IMPORTANT ISSUES FIRST

Your new Presentation Master or Victorinox Secure product is a highly modern electronic tool, which contains precision electronics. For the trouble-free operation of these parts, it is important that you observe the following instructions:

- Protect the product against moisture. Do not use any of the electronic modules in wet environments.
- Never clean the electronic modules with chemical cleaning agents.
- The surface of the fingerprint sensor can be easily scratched. Do not attempt, for example, to scratch dirt off of it, and never store it in pants pockets or handbags without protection.
- Please ensure that your fingers are always clean when using the fingerprint stick. Remnants from solvents, glues, oils or other chemicals may permanently damage the sensor.
- Only clean the stick with a moist (not wet) cotton cloth and never with a micro-fiber cleaning cloth. (Its fibers could damage the sensor.) Cloths intended for cleaning optical equipment, such as glasses or camera lenses, are appropriate for cleaning the sensor.



## GETTING STARTED

When using the biometric fingerprint stick, always connect and disconnect it carefully from the computer. Never use force or tilt it.

Always separate the stick from your Swiss Army Knife before plugging it into your computer. If you do not do so, the weight of the Swiss Army Knife could damage the stick or your computer (or rather, the port built into your computer).

When you connect your new biometric Victorinox Secure stick with your computer, four things might happen depending on the configuration of your computer:

- 1.) Your computer might request you to format your new Victorinox Presentation Master or Victorinox Secure stick. Do this under NO circumstances. The message appears because an update from Microsoft is missing from your computer. You can get this update from Microsoft free-of-charge. Please read page 8 of this guide for instructions.
- 2.) The application might automatically start, and you will then see a screen similar to Figure 1.
- 3.) A menu might appear, which asks if you would really like to run this application. You should allow this to happen. The application will then start.
- 4.) Absolutely nothing happens. In this case, try to start the application by double-clicking the file Secure.exe in the root directory of your stick. If this does not work, please contact your System Administrator.

**CAUTION:** If you are not able to start the application then possibly you do not have the associated rights for this. Contact your System Administrator in this case.



## FINGERPRINT RECOGNITION

The application must first be given a user password and at least two or more fingerprints. The password must be entered twice. In addition, the Windows User will be required for the Windows Look feature.

Please consider that you must be able to change the Windows User and Password, if you were to change these settings for your computer. If you forget this and have opted to login to your computer using the biometric stick, your stick will no longer be able to log you onto your computer properly.

The first thing you need to do is provide a stick password in the entry field. You must enter it twice, so that the application can verify it. [Figure 1]



Figure 1



The password must be at least 6 characters long, with at least one number, one letter and one special character.

When the password is the same in both entries, a green check mark will appear next to them. [Figure 2]

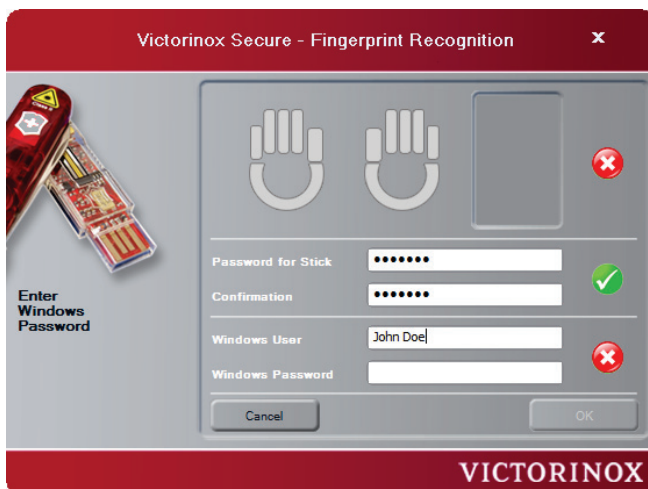


Figure 2

Next, enter your current Windows User Name as well as the associated password for your Windows system. This is required for logging in with Windows using fingerprints. [Figure 3] Pay careful attention to upper and lowercase letters.

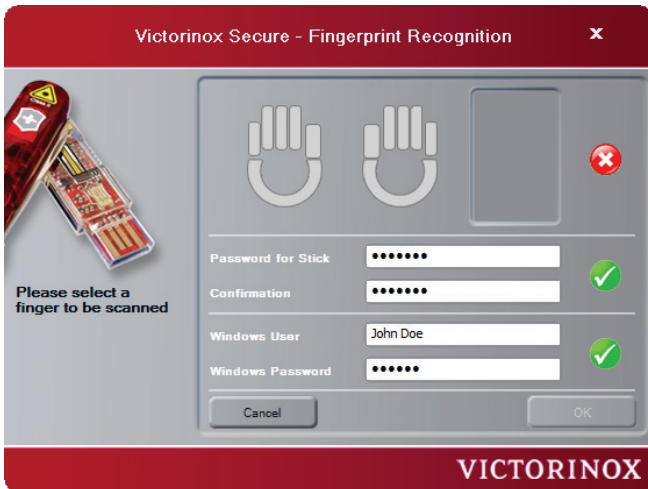


Figure 3

Next, to register a fingerprint, select the corresponding finger on the image using the mouse. [Figure 4]

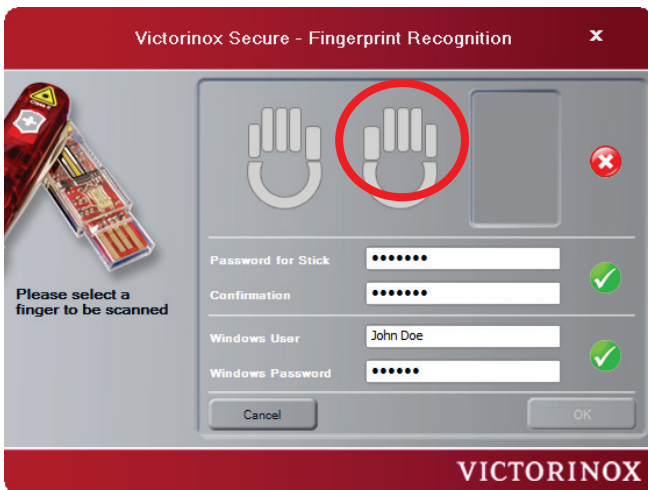


Figure 4

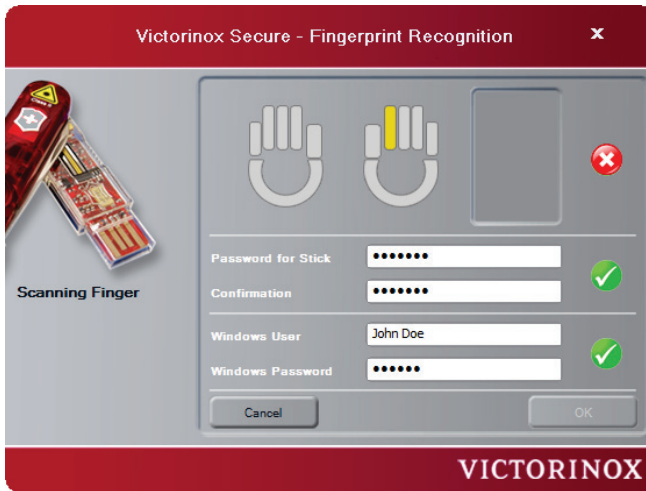


Figure 5

If the finger is yellow, that means that finger has been selected for recognition. Subsequently, the application will wait to scan your finger using the fingerprint scanner integrated into the USB stick. [Figure 6]

**Caution:** Please be careful to avoid applying excessive force to the sensor when scanning your finger. A touch is sufficient.

The usage of the fingerprint scanner may require some practice. Allow your finger to be scanned slowly and evenly. To do this, place the first joint of your finger over the sensor and pull it back slowly, so that the fingertip slides completely across the sensor.

**Tip:** Lay your finger lightly on the sensor and leave it there for about a second before pulling it across the sensor. This allows the sensor to adjust to your finger.

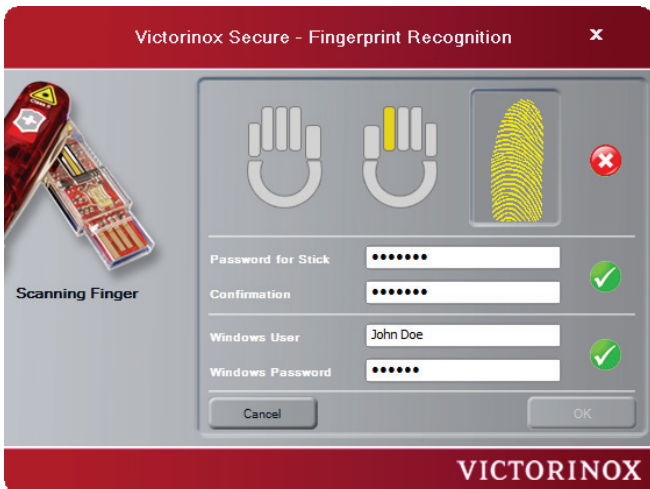


Figure 6

Repeat this procedure until the fingerprint image turns greens.  
[Figure 7]

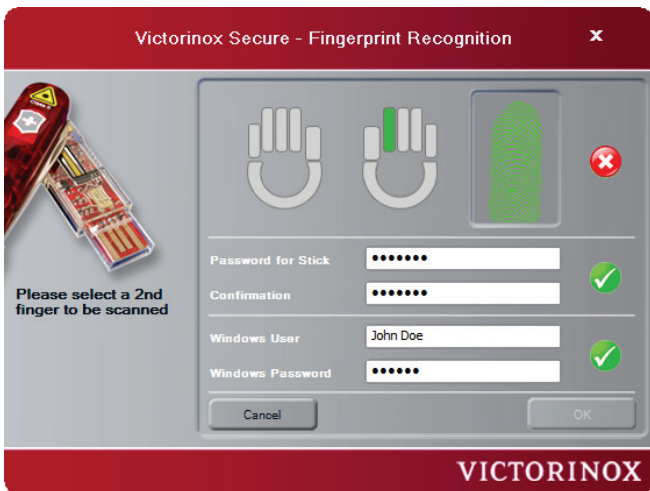


Figure 7



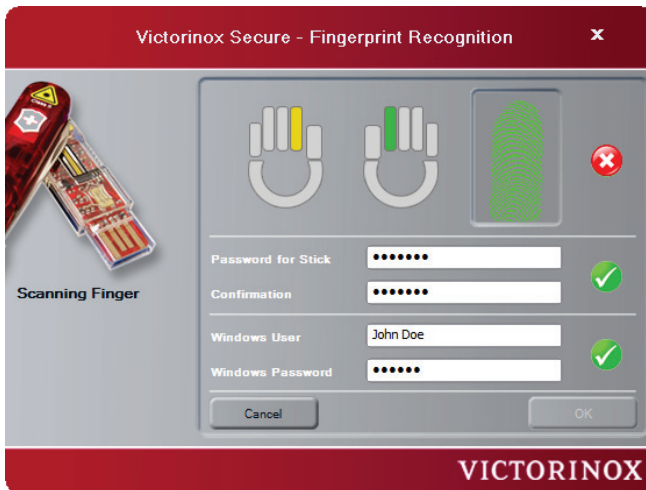


Figure 8

You may repeat this procedure for each finger. At least two fingerprints are required.

In order to recognize the second finger, select the corresponding finger on the image [Figure 8]. We recommend using the right and left index fingers, since this has proven practical depending upon whether the USB stick is on the left or right of the keyboard.

We recommend that you allow at least two fingers to be recognized for each hand.

If you would like to allow another person to access your stick using a fingerprint, you will need to allow their fingerprints to be recognized. The hands on the login screen depict 10 storage slots, which may be used for various fingerprints. These may be your ten fingers or six of your fingers and four fingers of your partner or any other authorized person.

Up to ten people may access the data by storing one fingerprint for each of them.

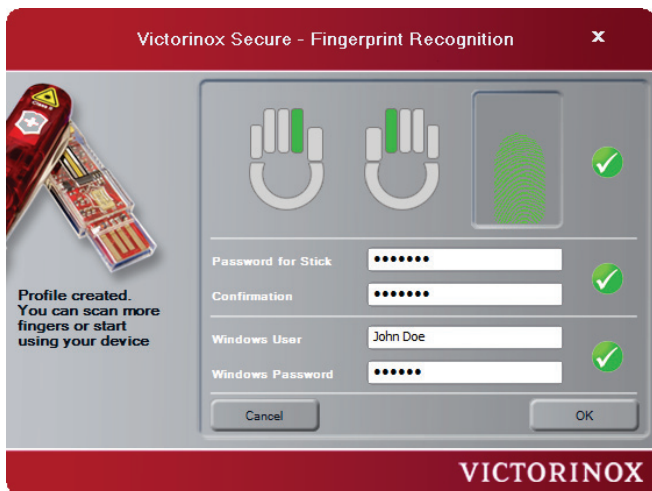


Figure 9

Now, allow your finger to be scanned slowly and evenly. You can see the result of each scan immediately.

Always repeat this procedure using the same finger until the image of the finger turns green. [Figure 9]



Figure 10

If needed, you may scan up to ten fingers.

After all three green check marks have appeared, the OK button will appear and you can conclude the creation of your profile by clicking on this button.



## LOGIN SCREEN

After you have successfully created your profile, the identification screen [Figure 11] will be displayed.

Once you have logged in by means of a fingerprint or the master password, you may use your biometric USB 2 stick.

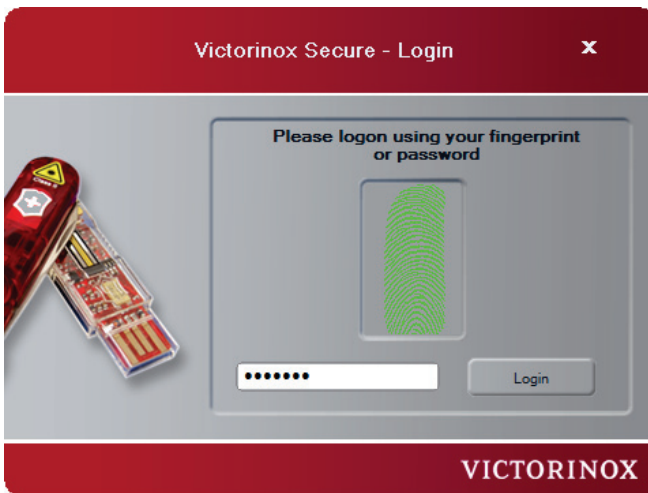



Figure 11


The next screen after logging in is the initial screen. [Figure 12]


It may be several seconds before the next screen appears, depending upon your configuration and the existing, encrypted drives. While it is starting, the application will also open any existing number of encrypted drives, corresponding to your settings.



## THE CAPTION AND THE NAVIGATION BAR

**Button**  The computer will be locked by clicking this button as if one had similarly used the **CTRL-ALT-DEL** feature.

**Button**  This button will take you directly to the Victorinox support web page. Additional guides are available for you there, as well as any potential updates.

**Button**  Opens the About dialog.

### The Navigation Bar:

The Select Drive menu is indicated by the two graphic markers and the active drive is indicated in yellow. In order to select another drive or USB stick, you need simply select it from this list using the mouse.

Additionally, the **Sync All button**, which executes a synchronization cycle based on the preset directories and options, is always located in the left bar. [Figure 11]

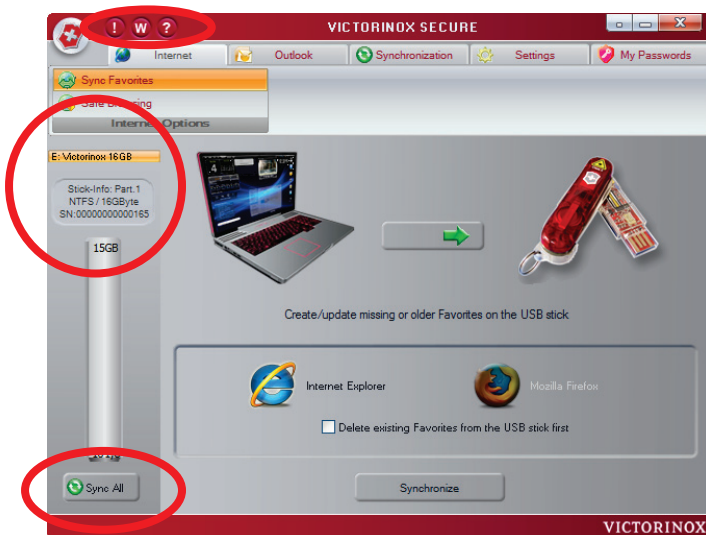


Figure 12



## INTERNET FEATURES

All of the features that affect the Internet use featured on these screens.

In this context, we would like to point out that the Safe Browsing software feature made available here does NOT enable anonymous surfing on the Internet (since this has been forbidden in many countries according to new legislation), but rather permits surfing without leaving any traces behind from the viewpoint of the computer. This means that your Internet provider is able to store your IP address, even when you use this feature.

The use of the Safe Browsing feature means that no data or information about your Internet activities is left behind on the computer when this feature is active.

## SYNC FAVORITES

The ***Sync Favorites*** entry is found on the Internet screen [Figure 12] in the first submenu. With the help of the selection button, you can determine the direction of synchronization: to the USB stick, from the USB stick to the computer or in both directions at the same time. Entries missing on the other side will be completed thereby.

The application automatically recognizes which browser you have installed. However, if both Internet Explorer and Mozilla Firefox are found on your computer, you may select the browser to which the settings should be applied by clicking the corresponding buttons.

When you have activated the ***Delete existing Favorites from the USB stick first*** checkbox, all of the existing entries under Favorites will be deleted during the next synchronization cycle.



Using the **Synchronize** button, the synchronization cycle will be started according to the settings.

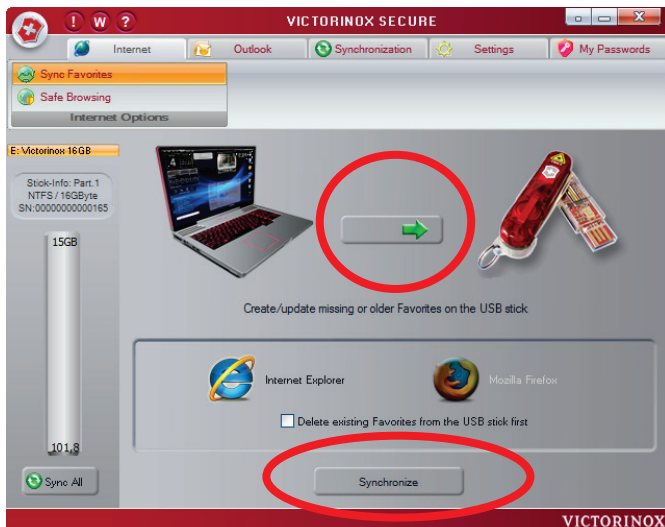


Figure 13

Please note that by clicking Synchronize all of the previously saved favorites may be deleted from the USB stick. (Depending on how “Delete existing Favorites from the USB Stick first” has been set).



## SAFE BROWSING

If you have checked the Activate Safe Browsing checkbox [Figure 14], Internet log files will not remain on the computer. This also means, however, that cookies cannot be permanently stored on your computer. Additionally the History feature will no longer be available, meaning that history cannot be traced.

If you would like to continue using these features, you also have the option of selectively deleting Internet traces from the Delete Local Internet Log Files menu item.

If you would like to delete the Internet traces that you have stored on the USB stick then you can do this using the “Delete Internet log files from USB stick” menu item.

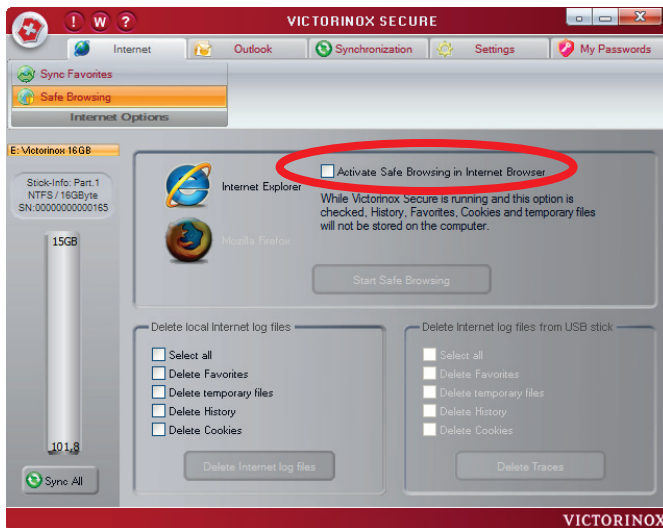


Figure 14





---

## OUTLOOK MENUS

Under the Outlook menu, you will find two different Outlook options: Mobile Outlook Express and a second submenu for the Outlook included with the Microsoft Office package. You may use the features corresponding to your configuration as they correspond to your installation.

The Outlook features enable you to synchronize important Outlook information, such as your emails, contact information, and calendars between two computers. With these features, you can also carry this information with you and have access to it using other computers, such as accessing your stored Outlook information in Internet cafes.

The backup feature is an additional feature. With your biometric stick, you can also create backups of your Outlook information simply and securely.

## OUTLOOK EXPRESS

The quantity of features in Outlook Express is intended for typical private usage. It does not have any Groupware and Unified-Messaging features, in contrast with Outlook, however can access news features. Outlook Express is present with most versions of Microsoft Windows as a feature. Normally, Outlook Express is only used when Microsoft Office has not been installed. Until now, Microsoft Office has included Outlook.

The Outlook Express features made available in this application automatically backup the entire Outlook Express database. When the data is restored, the entire database is recreated. Selective backup and restoration is only possible with Outlook. With Outlook Express, the complete contents of the profile are backed up and restored.



## BACKUP TO USB STICK

In order to be able to backup data from Outlook Express, the corresponding account must be selected first. [Figure 15]

You may, of course, select multiple accounts, if such exist.

By clicking the Create Backup button, the backup process is started and saved to the USB stick.

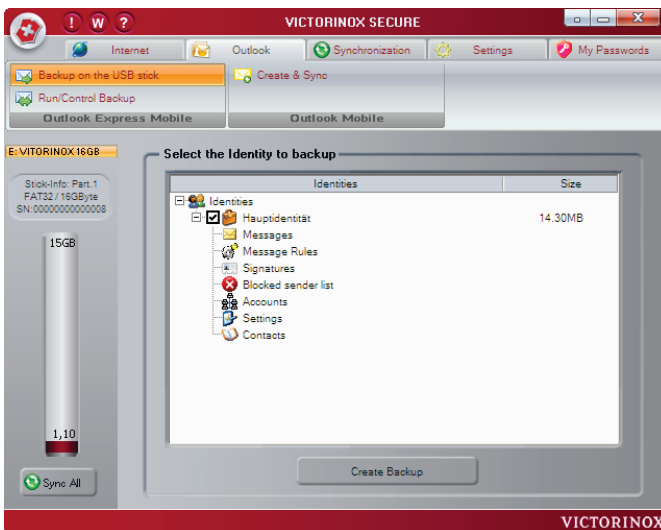


Figure 15

**Caution:** Please note that your backup is only protected from access by third parties when you have created it on an encrypted drive. For more details, read the Encrypted Drives section.



## RESTORING AND MANAGING BACKUPS

Of course, at some point a backup may need to be restored. To do this, select the corresponding backup and restore it by clicking the Restore button. [Figure 16]

Backups that are no longer needed can be simply deleted by selecting the backup and then clicking the Delete button.

Outlook Express can also be comfortably started using the Run Outlook Express button.

This, of course, assumes that Outlook Express has been installed.

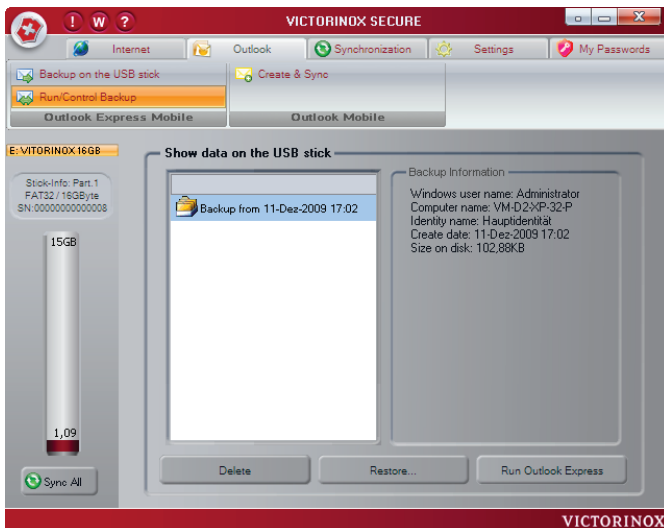


Figure 16



## MICROSOFT OUTLOOK

Outlook is primarily the client for Exchange Server, however, it may also be used without Exchange Server.

## CREATE & SYNCHRONIZE

In order to be able to backup data from Outlook, the corresponding profile to be backed up must be selected first. This can be done with the help of the Add Profiles button. [Figure 16]

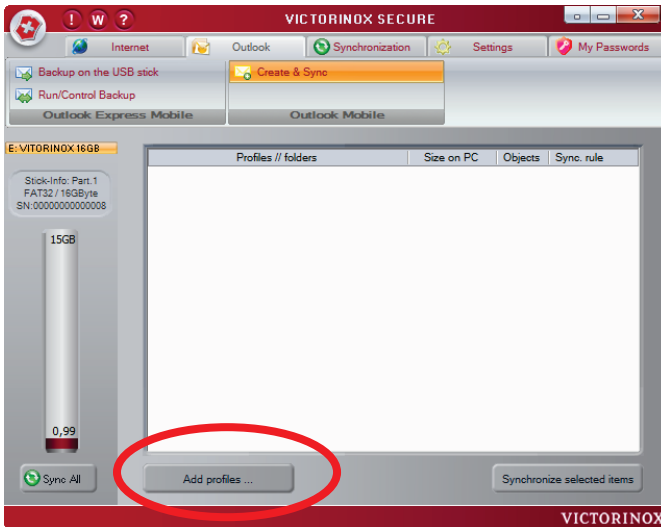


Figure 17



The screen [Figure 17], which is then opened, offers a selection of profiles on the left side for synchronization. On the right side, the determination is made whether this process involves a new backup or a pre-existing, which may have been created by another computer.



**Figure 18**

The profile is added to the list of profiles to be backed up by clicking the OK button. [Figure 18]

A “Profile Pair” refers to the connection between your biometric USB stick and an Outlook profile. If you use several Outlook profiles (on various computers, for example), then you can create several profile pairs.

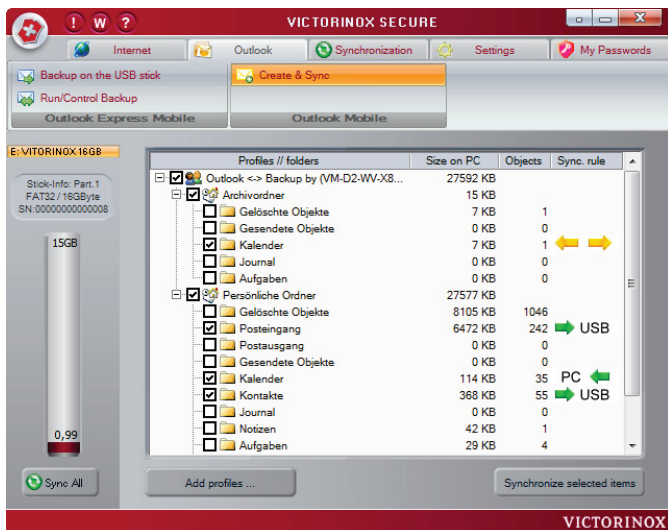


Figure 19

The direction of object synchronization is determined with the help of the Sync. Rules control. If both direction simultaneously is selected then missing objects on both sides will be exchanged.



## OVERWRITING OUTLOOK INFORMATION

With the help of the Add Profiles button, existing Outlook backups can overwrite the local Outlook information on other computers. To do this, simply select the corresponding backup from the USB stick [Figure 20]. The name of the computer that created the backup is displayed in parenthesis (in this example, VM-D2-WV-32-UO).



Figure 20



## DELETE OUTLOOK PROFILES

In order to delete a profile that is no longer needed right-click on the top-most item for that profile.

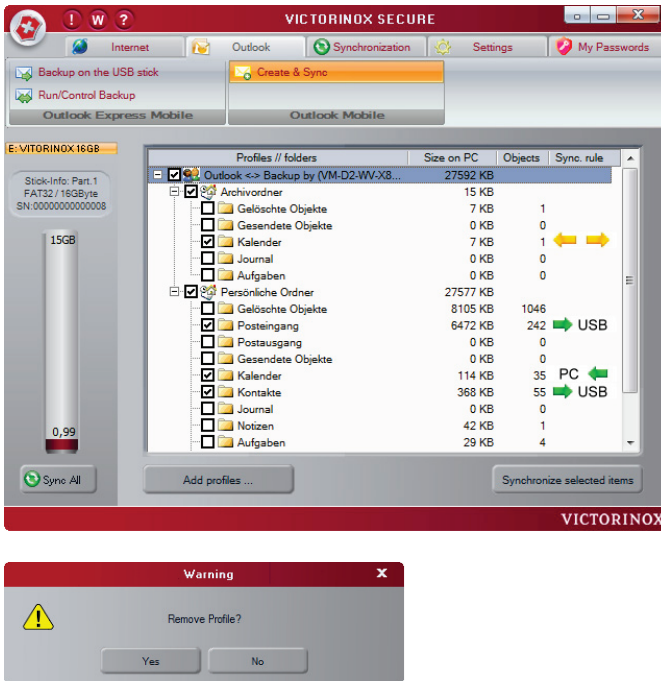


Figure 21

Please note that, when you delete a profile pair, you will also delete all of the data stored on the USB stick along with it.





---

## SYNCHRONIZING

Data synchronization enables you to backup your data on the USB stick as well as synchronize it with other computers. For this, you may use your personal My Documents working folder, as well as any other folder on the local computer or any network drive.

**Caution:** If you synchronize data then it will be transferred with the help of your USB stick from one computer to another.

Data on your USB stick is only protected from access by unauthorized people, if you store it on an encrypted drive. For more details, read the Encrypted Drives chapter.



## YOUR DOCUMENTS

Your own documents can be selected from the local computer as well as from the USB stick. In order to switch between the local computer and the USB stick, click on the Notebook or USB stick icons at the top.

Select the desired folder using a check mark.

Before you click the Synchronize button, use the arrow buttons to set whether you want to only write to the USB stick, or replace data on the computer, or want to synchronize both at the same time.

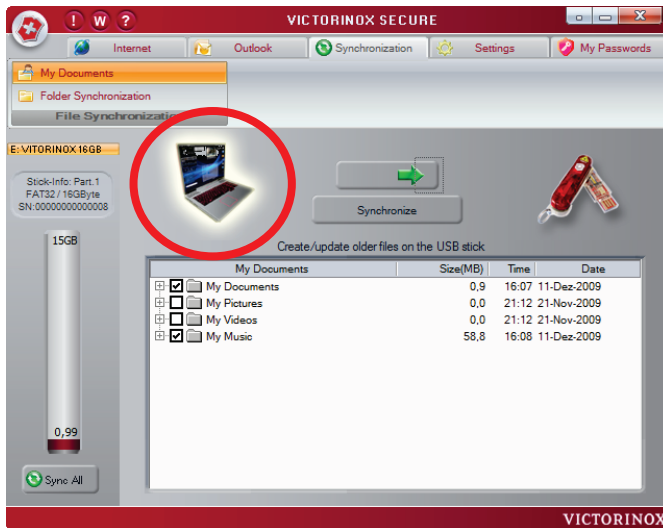


Figure 22



## FOLDER SYNCHRONIZATION

In order to be able to synchronize additional folders or files, you can open a new screen, with which you can select the corresponding folder, under Folder Synchronization [Figure 23] by means of the Add button.

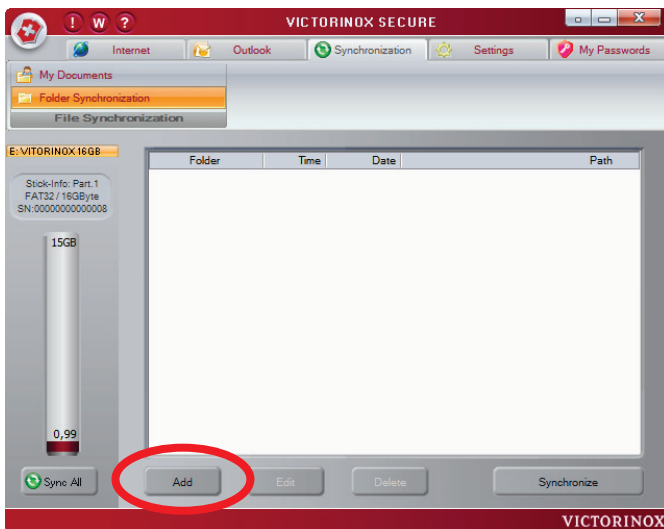


Figure 23

As can be seen in [Figure 23], you can also specify a number of parameters when selecting folders, such as whether the folder should be transferred and stored as a ZIP file, or if any potentially pre-existing folders should first be deleted from target storage.



The complete Desktop content is synchronized using the Desktop icon. To do this, you need to click the red cross next to the Desktop icon.



Figure 24



## SETTINGS

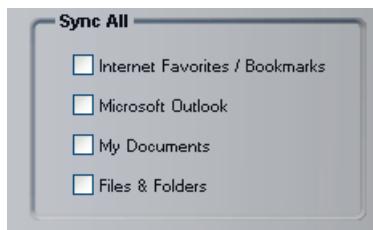
All of the settings that affect your biometric stick have been collected in this menu. It is very important that you first create your encrypted drives from here. Data that you store on your biometric stick is only secure when you save it on an encrypted drive.

Thereby, you have the option of storing two types of data on your stick: that which all users can access, and data that only you or a very limited group of people defined by you can access. Data that is stored in the encrypted drives is also still encrypted using the AES 256 bit procedure. This means the data has been encrypted so that if a specialist could extract the memory chip from your stick, they will not be able to access it.

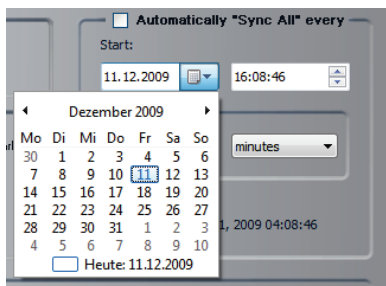
And when you now ask, if we, the manufacturer of this USB stick might be able to read your encrypted data, the answer is: NO. Even we can't do that. For this reason, you should be very careful about how you treat your stick, because even we cannot restore it in the event that you forget your password and your fingers.

## SYNCHRONIZATION SETTINGS

The settings in the Sync All group determine what should be transferred during synchronization. Simple selection using the checkboxes is enough. The information will be stored and used for the next synchronization cycle.



Additionally, you can activate the automated synchronization cycle, and determine the initial starting time including data and the synchronization interval. If, for example, you want to set the automated synchronization to start next Monday, every other day at noon:



With the help of the calendar, select the next Monday and set the start time to 12:00:00.

Since the synchronization cycle should run every other day from that date, an interval of 2 days needs to be entered.

Furthermore, from this screen you can set the language as well as the Windows login settings.

Language – In principle, the application assumes that the language used by Windows is the desired language, regardless of whether that is German, English, French, Italian, Spanish, Russian, Chinese or Japanese. However, if the operating system does not use one of the eight listed languages, the application will start in English by default. Using the Language menu item [Figure 25], you now have the option to overwrite this selection and thus use the application in German, even if the computer has been installed with an English operating system.

## SECURITY SETTINGS

Using Lock PC When Stick Removed [Figure 25], you know that your computer will automatically be secured when you remove the stick. After the removal of the USB stick, the computer can only be re-activated using the Windows password or fingerprint (after re-inserting the USB stick).

If you uncheck Enable All Warnings [Figure 25], the Victorinox Secure will only show you the most important warnings. Above all, this setting is appropriate for all experienced Victorinox Secure users.

If you check Lock On Screensaver [Figure 25], the computer will also be secured when the screensaver starts. That means that as soon as you move the mouse or press a key, the login dialog will appear.



Due to technical considerations, the Fingerprint Logon option is only available for computers running under Windows Vista 32 Bit or Windows 7 32 Bit. For this reason, this feature is hidden when the application is running under Windows XP or 64-bit operating systems.

If you check Fingerprint Logon [Figure 25] then you can login to Windows using your fingerprint.

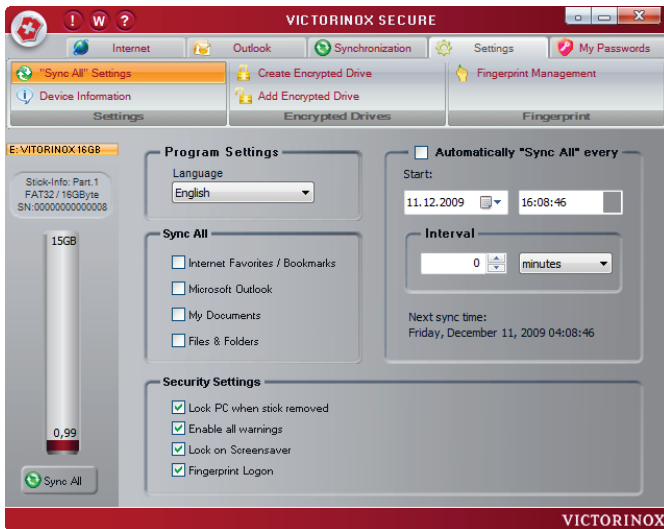


Figure 25



## WINDOWS LOGIN USING A FINGERPRINT

Fingerprint logon simplifies the everyday use of Windows passwords. After Fingerprint Logon [Figure 25] has been set, you will see an additional user icon [Figure 27] once you try to switch users [Figure 26].

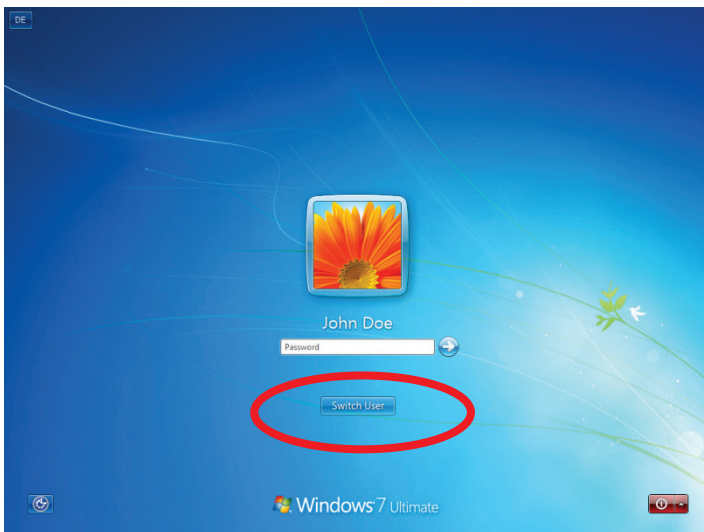
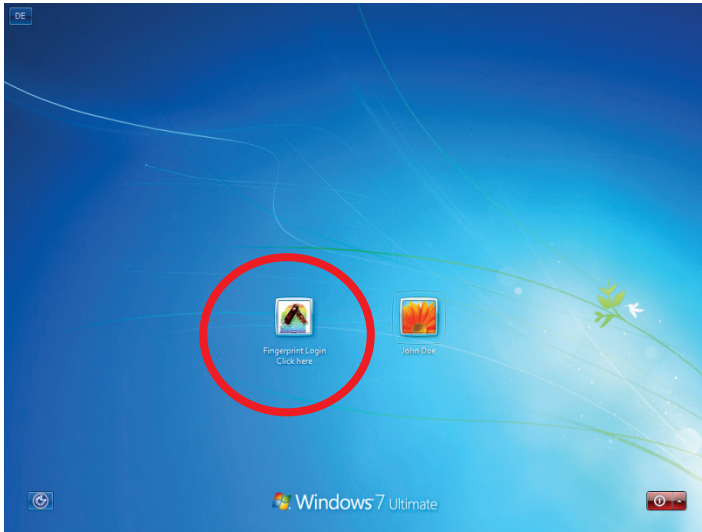


Figure 26

If you now select Fingerprint Login [Figure 27], a new login dialog [Figure 28] will appear.

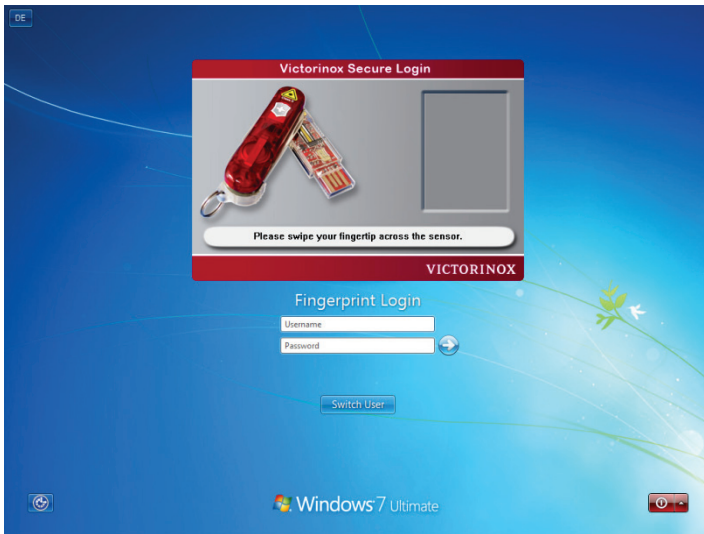




**Figure 27**

You now have the option of entering your User Name and Password, as always, or simply logging in using your fingerprint. [Figure 27]

For logging in using a fingerprint, you simply swipe your pre-registered finger across the scanner (as you did when registering your fingerprint).



**Figure 28**

If there is an error or the fingerprint is not recognized, the image of the fingerprint will turn red [Figure 29]. Afterwards you will be asked to scan a finger again until the system has recognized your fingerprint and logged you in. [Figure 30]

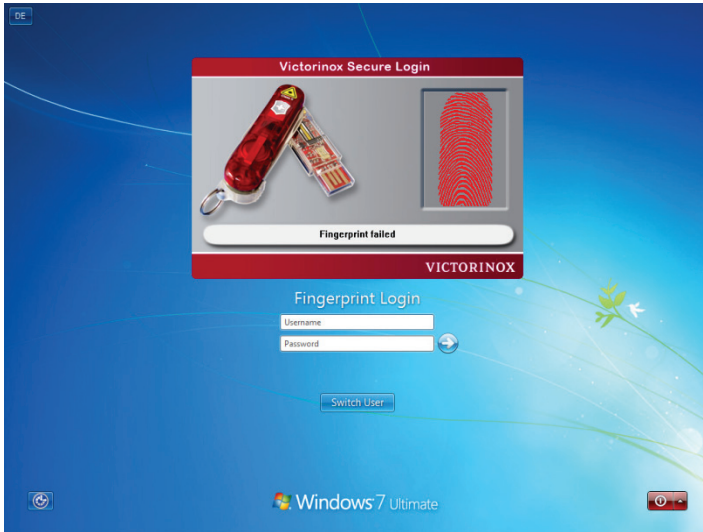


Figure 29

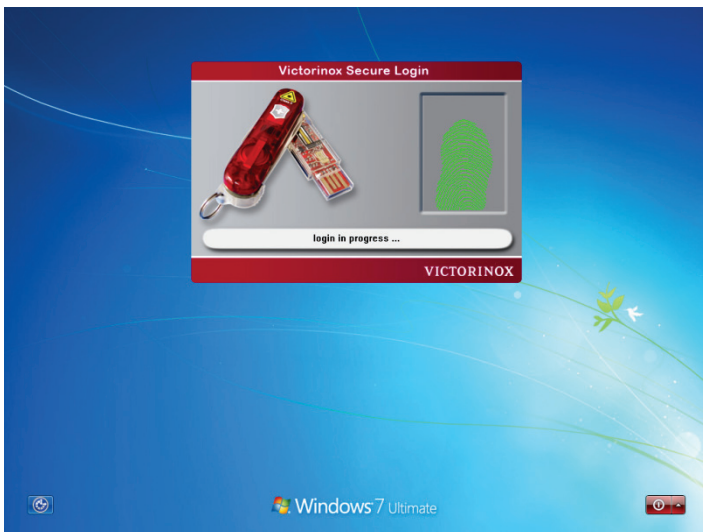


Figure 30



## DEVICE INFORMATION

The Device Information screen displays several pieces of information, such as the serial number of the USB device and statistical information about how the storage space is being used. [Figure 31]

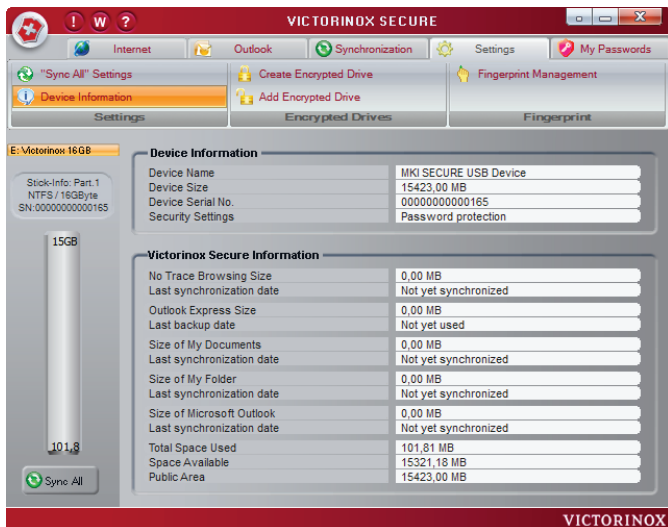


Figure 31



---

## ENCRYPTED DRIVES

With the Victorinox Secure product, you have a tool for creating secure, virtual drives that can only be opened using the right password or fingerprint. These drives are encrypted using AES 256 and considered very secure.

The actual storage space for these virtual drives is located on your USB stick, however, is displayed by Windows like a completely normal drive. Once a drive has been started, you can use it with Windows as if you had an additional drive.

Please keep in mind that even virtual drives require real storage. This storage is located on the USB stick under the Virtual Drives directory. Later, you will find files in this folder with “xsvd” extensions. Each of these files reserves physical storage space for each virtual drive. If you were to delete one of these files then you would also be deleting the corresponding encrypted drive and consequently all of the data stored in it would then be gone.

## CREATING A DRIVE

To create an encrypted, virtual drive, you first specify the name of the drive in the entry field.

Of course, the password for this new drive should not be forgotten. Please try to use passwords, which you will be able to remember, but which should also be “secure”. If you forget your password, you will no longer be able to access the data on that drive. During application development, we specifically avoided these types of features for reasons of security.

The specification of the size of the new drive should be determined carefully in advance. If you want to use this drive for lots of images or other large files then it should be significantly larger than if you wanted to primarily secure text documents. The minimum size is 3 MB.



The maximum is only limited by the space available on the USB stick. [Figure 32]

Please note that all of the storage space that you allocate for this new secure drive is immediately reserved, even when the drive itself is still empty.

Example: If you were to create an 8 GB drive on a USB stick that had previously indicated 10 GB free, then after the creation of the drive only 2 GB would remain available, even if the encrypted drive were still empty.

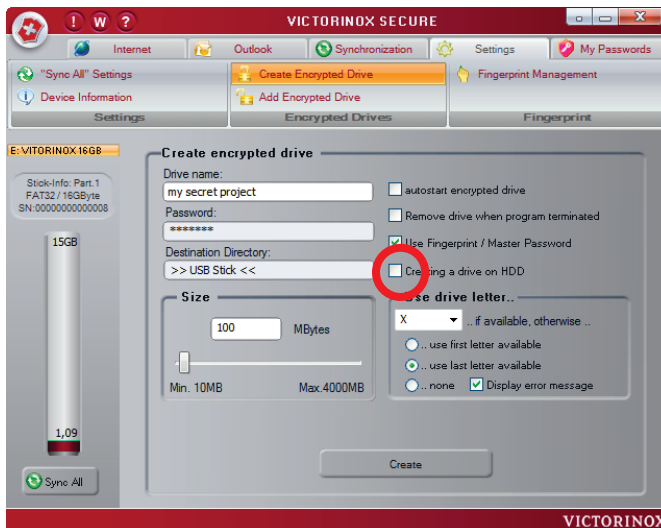



Figure 32

**Caution:** In order to create a secure drive, we recommend not using the option “Use Fingerprint/Master Password”.

Use a different password than the Master Password with a minimum of 7 characters or more.



Of course, encrypted drives can also be stored on a hard disk. To do this, set the checkbox (indicated by the red circle) and subsequently a little icon  will appear after Destination Directory. By default, the file made available for the encrypted drive is stored in the Windows user directory under “\AppData\MKI\Secure Drives”.

You can then determine a different location for this file using the icon. Clicking on the folder icon opens a selection dialog.

After you have selected all your settings and checked them, the new drive will be created when you click the **Create button**. Depending on the size, this may require anywhere from 10 seconds to several minutes. As this process is running, the yellow progress bar will move towards the right until it reaches 100%.

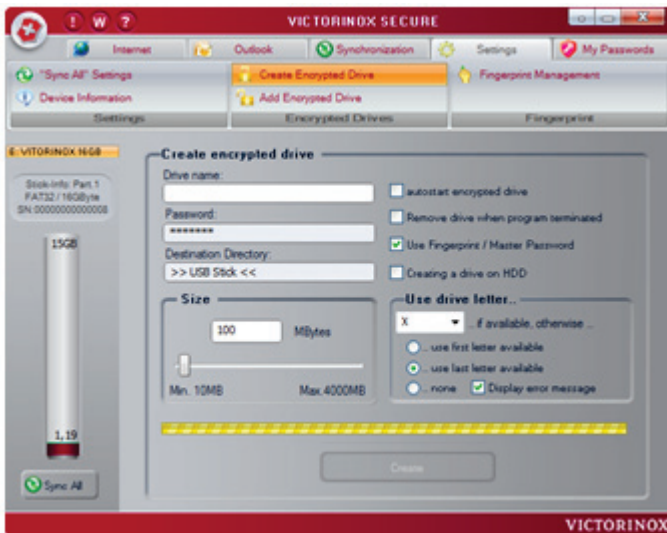
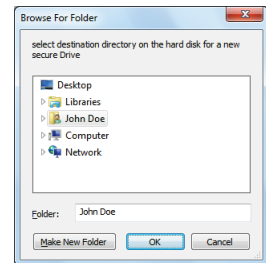


Figure 33

Depending on the size of the encrypted drive that you create, this may require anywhere from a few minutes to several hours. The amount of



time required depends not only on the size of the drive, but also on the computing power of your computer.

After the drive has been successfully created, it will appear in the list of virtual drives under Add Encrypted Drive. [Figure 34]

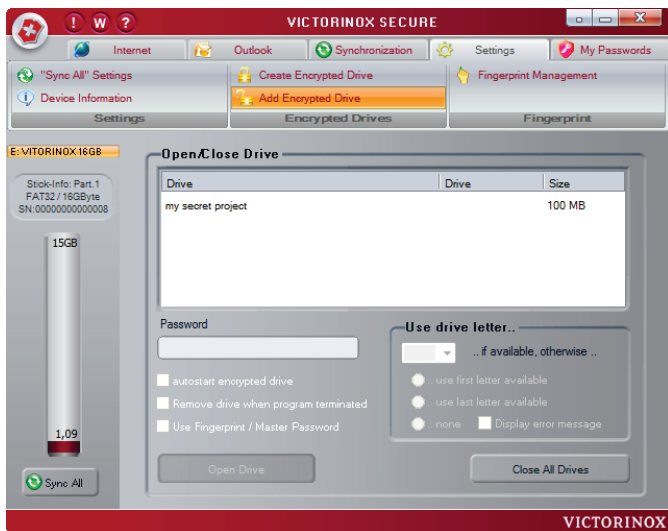


Figure 34

From this screen, you can now set the options for any drive which has already been created as you would like.





## STARTING A DRIVE

To start a drive, you must select it from the list of drives using the mouse, enter the corresponding password in the password field, and click the Open Drive button. [Figure 35]

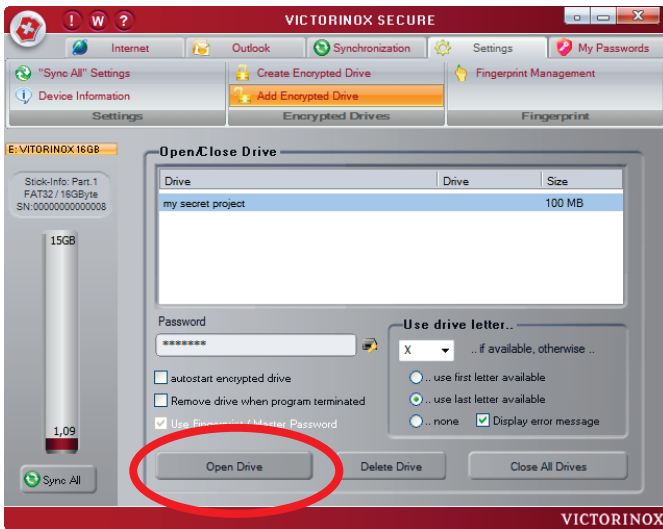
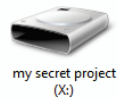


Figure 35

After the drive has been successfully started, it should also be listed under My Computer.



You can now use this drive as if it were your own hard disk. However, you should also keep in mind that you have to close the drive before removing the USB stick.



## CLOSING A DRIVE

The best approach to closing an open drive would be to select the corresponding drive from the Encrypted Drives screen and then click the Close Drive button. [Figure 36]

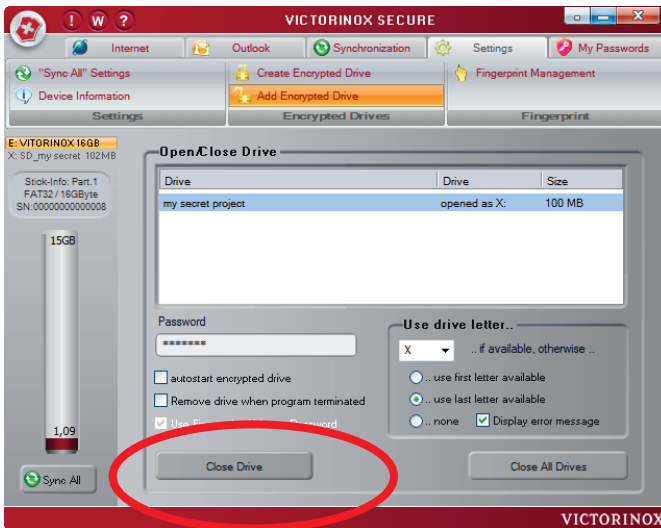


Figure 36



## DELETING A DRIVE

When encrypted drives are no longer needed, you may delete them... To do this, select the corresponding drive in this list and use the Delete Drive button. [Figure 37]

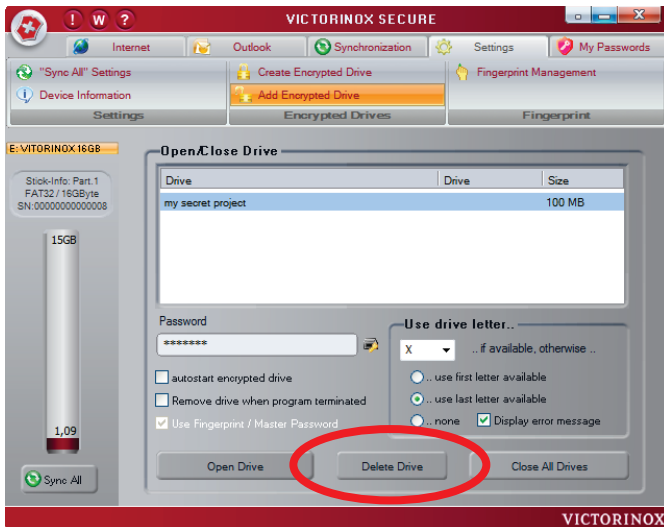


Figure 37



## MANAGING FINGERPRINTS

Managing fingerprints is similar to the fingerprint recognition procedure (see the Chapter entitled Fingerprint Recognition). Initially, you will see the current state. From here, fingerprints can be added, deleted or modified. To select the finger that you would like to edit, it must be selected using the mouse. The selected finger is indicated in yellow, as seen already under Fingerprint Recognition.

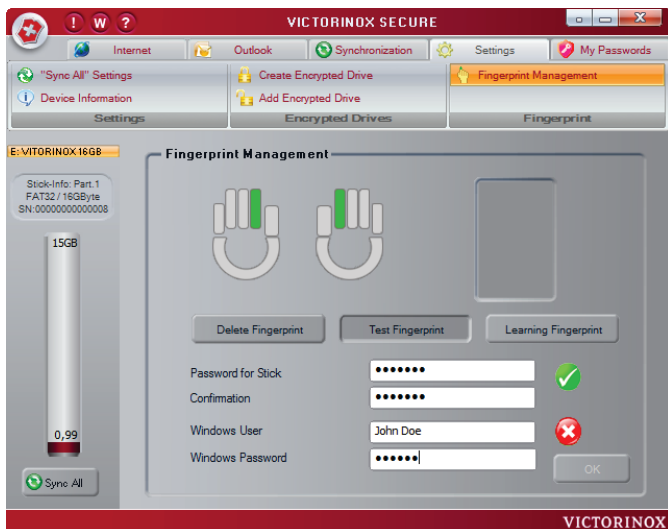


Figure 38

In addition, the password for the USB stick can be changed, whereby the new password must be entered twice. The password must correspond to the password rules as described in the Fingerprint Recognition chapter.

The Windows User can be changed using the Windows User entry. The application will check if the specified user exists and correspondingly



indicates this with either a red or green check mark.

All modifications are saved by clicking OK and applied immediately. However, this button will only become active when no errors have been made.

## THE PASSWORD MANAGER

The My Password screen [Figure 39] is divided into fields that list the passwords as well as those in which passwords can be added, modified and deleted. A filter for the selected category can be set using the Category combo-box button. Only those entries will appear in the list of passwords that correspond to the selected category.

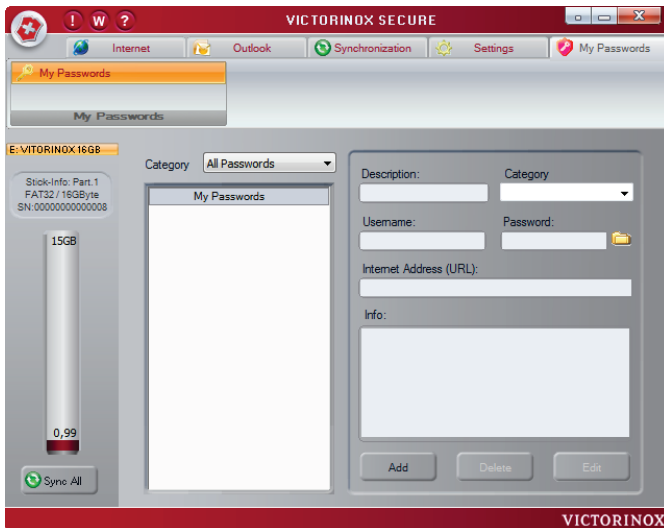


Figure 39



## ADDING A PASSWORD

In order to be able to add a new password, first click on the Add button as indicated in [Figure 40].

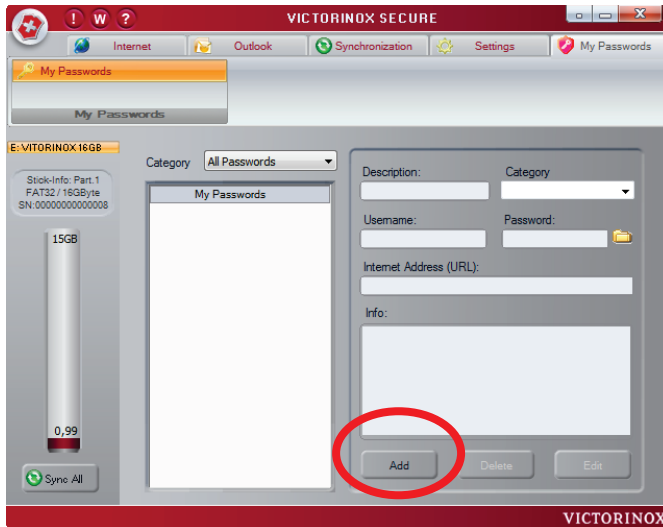


Figure 40

Fill in the corresponding fields, such as Description, Name and Password. Either you have already created an appropriate category or, if not, you will now create a new category, by simply entering the name of the new category in the Category field.

The Info and Internet Address fields are optional and do not need to be entered.

To save the new password, click the **Accept button**.

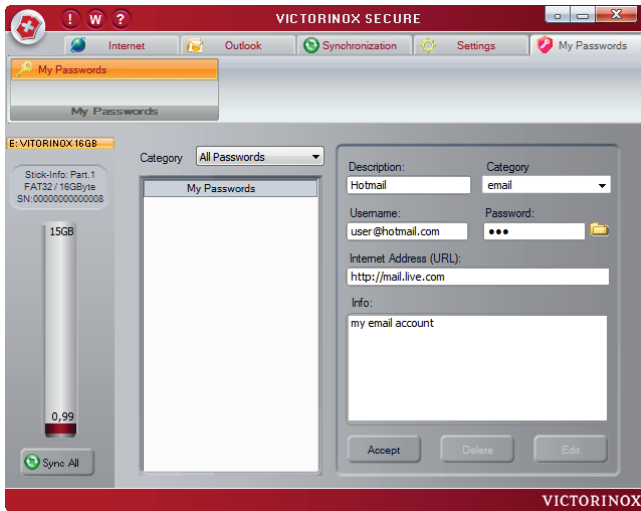


Figure 41

After the new password has been successfully saved, you will see it in the list of passwords as in [Figure 42].

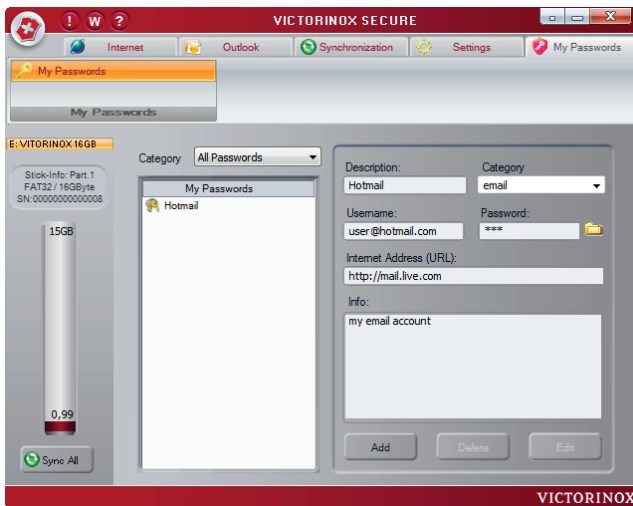


Figure 42



## CHANGING A PASSWORD

If you want to modify or supplement an existing password, select it from the list of passwords. Once the password has been selected, the Delete and Edit buttons become active. By clicking the Edit button, the entries on the right side of the screen that are associated with the password will be activated.

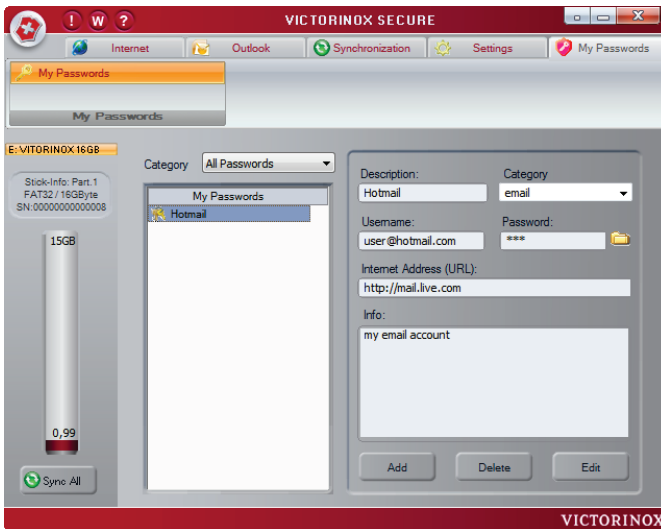


Figure 43

After you have completed your changes, store them by clicking the Accept button [Figure 44].



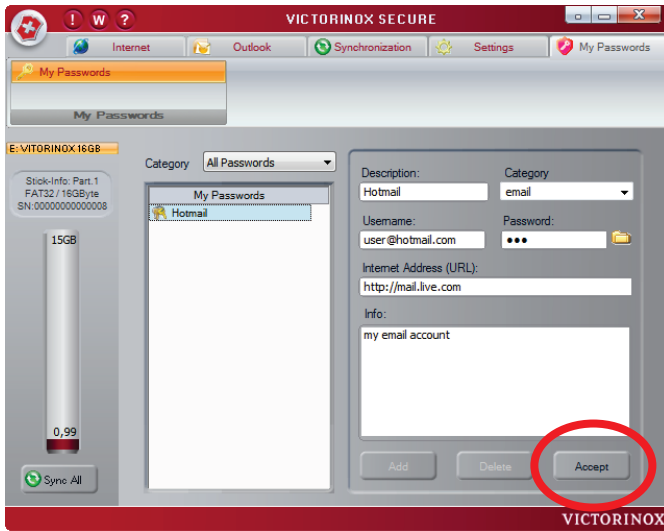


Figure 44

## DELETING A PASSWORD

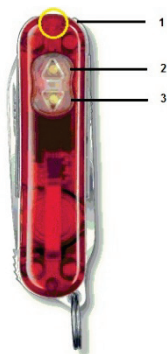
In order to delete a password from the list, select it and click the Delete button.



## THE BLUETOOTH MODULE

This module is available with the Presentation Master and Presentation Master Flight products and is found on the back of the knife. It has a WIPP button with two position (Previous / Next) as well as a red power LED.

## CONNECTING THE BLUETOOTH MODULE



Only the Presentation Master and Presentation Master Flight products have the Bluetooth feature.

Bluetooth Controls:

1. Power LED
2. Next WIPP button
3. Previous WIPP button

In order to be able to use the Bluetooth module with your computer, you must first connect it with your computer. Since this requires a lot of transmission power, it is important that you use a new battery when performing this step. Your Bluetooth module can also work with an older battery for several hours, but connecting it with a computer is only possible when using a new battery that has sufficient capacity.

You should ensure that Bluetooth has been activated on your PC. Start the Bluetooth application. (Please note that you should not be using two different Bluetooth pointing devices at the same time. This can lead to confusion. If you are already using a Bluetooth mouse then you should unregister it before using the Presentation Manager Bluetooth module. (Our tests have indicated that many Bluetooth mice, such as the Microsoft Bluetooth Notebook Mouse 5000 can be used without causing any problems.) You should have received this application



together with your PC. It will differ depending on the model of your computer. We recommend the usage of the Microsoft Bluetooth stack. However, the module can also work with other compatible Bluetooth stacks. You will find the User's Guide on how this application is used in your computer's manual.

Use this application to set your computer to search for new Bluetooth devices. As soon as the application makes its request that you activate your Bluetooth device or place it in pairing mode, insert the battery into your Bluetooth module. (Check the pole orientation of the battery and place the "+" pole down towards the knife's shell, so that you see the "-" pole.)

Now, press the Down button until the red LED blinks once. The module has been activated in discovery mode.

**Caution: If you do not complete the configuration within the next 5 minutes, the module will automatically turn itself off.**

Have the Bluetooth application on your PC search for new devices. You should find a BTM 420 module (where BTM stands for **B**lue**T**ooth **M**ouse).

As indicated by your Bluetooth manual, the application will now connect your PC with this module. If you are requested to enter a security code, select the option, "No Security Code Required".

Your PC should now be connected with the Bluetooth module.



## WORKING WITH THE BLUETOOTH MODULE

The Bluetooth module emulates the right and left mouse buttons. With them, you can remotely trigger all of the actions that you would normally be able to achieve using these mouse buttons.

In order to browse backwards and forwards in a PowerPoint presentation, simply press the up and down buttons on your Presentation Master.

### **Activating and Deactivating the Module:**

Click the Up button for 3 seconds: The LED will blink once and the module will deactivate itself.

Click the Down button for 3 seconds: The LED will blink once and the module will activate itself. Now click either the Up or Down button once and the module will automatically connect itself with your computer.

**Caution: The module will automatically deactivate itself after a 5-minute period of inactivity.**

### **Reactivating:**

Click the Down button until the LED blinks once; the module will activate and connect with your computer automatically.

### **To connect the module to another PC:**

Click the Down button until the LED blinks three times; the module will activate and switch into discovery mode automatically.



---

## BLUETOOTH PROBLEMS AND THEIR CAUSES

**Problem:**            **The computer does not find the Bluetooth module.**

**Solution:**            If Bluetooth has not already been activated on the computer, do that now.

If Bluetooth cannot be activated on the computer, although the switch or button are present, there are two causes for this behavior: either the function buttons driver has not been properly installed on the computer (to install it correctly, contact the support desk for your computer's manufacturer), or your device does not have an internal Bluetooth module, despite the presence of the Bluetooth button. In this case, your computer hardware will need to be upgraded. Contact the support desk of your computer's manufacturer.

**Problem:**            **The computer does not find the Bluetooth module although other Bluetooth devices operate properly.**

**Solution:**            If you use a Bluetooth mouse or a Bluetooth keyboard, deactivate it and try again. If that does not work, try inserting a new, type 389E battery in your Presentation Master and then try it again.

**Problem:**            **The Up and Down buttons on the Presentation Master have the opposite effect.**

**Solution:**            Open the Mouse application in Window's Control Panel and check or uncheck the setting, "Switch primary and secondary buttons".



## SUPPORT INFORMATION

You will find updates, additional product information and support on the Internet at the following address:

<http://www.victorinox.com/support/usb>

You can reach us at the following address:

VICTORINOX  
CH-6438 Ibach-Schwyz  
Switzerland

Phone: +41 41 81 81 211  
Fax: +41 41 81 81 511  
<http://www.victorinox.com>

In the USA:

Victorinox Swiss Army, Inc.  
7 Victoria Drive  
P.O. Box 1212  
Monroe, CT 06468

Customer Information 1-800-442-2706  
<http://www.swissarmy.com>



---

## NOTES AND LEGAL ISSUES

### **Exclusion of Liability**

The information provided in this guide as well as the underlying software was composed with the most care possible. The software and guide were checked repeatedly to the best of our knowledge and errors in good faith. However, we cannot completely exclude deviations or error in the guide and/or software. For this reason, we do not assume any liability for possible errors that might be contained in this description and in the software, or any consequences in connection with such, such as the loss of data, etc.

All information provided in this guide as well as the functionality of the software were regularly inspected and updates are made available on our web site, free-of-charge.

### **Copyright**

© Copyright 2009 Victorinox AG.

All rights reserved, in particular (even extracts) those of the translation, reproduction, transmission by copying or similar processes. Infringement obligates such persons to compensation for damages. All rights reserved.

Transmission and duplication of this publication, or portions thereof, regardless of means or purpose, are only allowed with the express written permission of Victorinox AG. The information contained in this publication may be modified without prior notification.

Microsoft, Windows, Microsoft Office, Vista, Outlook, PowerPoint, Outlook Express and Internet Explorer are registered trademarks of the Microsoft Corporation.

Linux is a registered trademark of Linus Torvalds in the USA and other countries.



Adobe and Acrobat are trademarks or registered trademarks of Adobe System, Inc. in the USA and other countries.

Intel and the Intel logo are registered trademarks of the Intel Corporation in the USA and other countries.

AMD and the AMD logo are registered trademarks of the AMD Corporation in the USA and other countries.

Bluetooth and the Bluetooth symbol are the property of Bluetooth SIG, Inc., USA, and have been licensed to Victorinox AG.

USB and the USB-IF logo are registered trademarks of the Universal Serial Bus Implementers Forum, Inc., in the USA and other countries.