

# Enterprise Deskside Support Services



CGI Corporate Office

## Laptop Encryption - User documentation

February 27, 2009



**Conseillers en gestion et informatique CGI inc.**

1350 René-Lévesque Blvd. West, 15th floor, Montréal, Quebec H3G 1T4

Telephone: (514) 415-3000

Fax: (514) 415-3999

---

**REVISION HISTORY**

---

Date	Version	Description	Author
2008-11-17	0.1	Initial document	Philippe Aubert
2008-11-19	0.2	Corrections	Philippe Aubert
2008-11-20	0.3	Corrections and change of structure	Vincent Carrier
2008-11-21	0.4	Corrections and modification of section 3.2	Philippe Aubert
2008-11-25	0.5	Modification of section 2.2	Philippe Aubert
2008-11-27	0.6	Modification of section 3.3	Philippe Aubert
2008-12-10	0.7	Minor structure changes	Philippe Aubert
2008-12-17	0.8	Modification section 2.3	Philippe Aubert
2009-02-23	0.9	Version change 5.35 Modification section 3.2	Philippe Aubert

---

**TABLE OF CONTENTS**

---

	Page
1 INTRODUCTION .....	1
2 OVERVIEW OF ENCRYPTED ENVIRONMENT .....	2
2.1 Installation .....	2
2.2 Logon to the system.....	2
2.3 Changes to the Windows environment .....	3
3 FREQUENTLY ASKED QUESTIONS.....	5
3.1 Is there any risk of losing my data?.....	5
3.2 How do I change my logon password?.....	5
3.3 How do I recover a forgotten logon password?.....	6
3.4 How to give access to my computer to another user? .....	8
3.5 What are all those advanced options on the POA screen?.....	10
3.6 How do I change my keyboard layout in the POA? .....	11
3.7 Will the files I send through e-mail or put on an external media be encrypted? .....	11

---

## 1 INTRODUCTION

---

Utimaco Safeguard Enterprise (SGN for short) is a powerful policy-based modular encryption and data security software product. It is managed centrally from a single console and is compatible with active directory.

This product is planned to be deployed on all mobile workstations belonging to CGI, as a measure to prevent data theft and it is important to be aware of every particularity of Safeguard and how it is implemented in the CGI desktop environment.

This document is meant to familiarize you with the day-to-day usage of this new system and understand the differences that are now present in your work environment.

The current production version is 5.35.2.7.

---

## 2 OVERVIEW OF ENCRYPTED ENVIRONMENT

---

### 2.1 Installation

---

Utimaco Safeguard will be installed on your computer by your local IT services. It may be done by a technician, or deployed automatically using a script. Once the installation is done and the system is properly configured, disk drives encryption will proceed automatically.

During the **encryption process**, it is important to note that you **can work normally**, accessing everything as usual including **files, network resources and all OS features**. If the PC needs to be shut down, **the encryption will then continue** at the next logon.

### 2.2 Logon to the system

---

Safeguard changes significantly the way you log on to your computer. As soon as encryption is complete, you will notice a different logon screen. This screen is shown before Windows is even loaded, and is known as POA (Power On Authentication). POA must validate your credentials at this point in order to unlock the Windows operating system.



Once unlocked, Windows will start normally, and as you also have access to Windows. Thus, POA should be considered as the new logon screen for users since a **pass through system** makes sure the typical **Windows logon** screen is automatically accessed when a valid user **authenticate from the POA**.

Therefore, in POA, you need to enter your **domain username and password** for a successful login. The **domain** should be the one that you normally log on to. The username to enter in POA is typically the same as the one you normally enter in the **Windows logon** before Safeguard was installed. However, this is not always the case, and even if the domain accepts more than one username alias, POA will take the default formulation. Normally, the username to use would be “**firstname.lastname**”, but some domains will require entering the **pre-Windows 2000 username** instead. For example, domain **AD.GIT.CGINET** will take the username in the form of “**Txxxxxx**”, where “xxxxxx” is the **employee number** (e.g. “T010203” for employee number 010203). Thus, if the native Active Directory username does not work, you should try your **pre-windows 2000 username**. Please note that as indicated below, there is a maximum number of erroneous password attempts.

If you make a mistake, an error message and a progress bar will appear. Your system will freeze during a certain delay, and this delay increases at each unsuccessful login attempt ( $N^3$  seconds, where  $N$  is the number of concurrent tries). This limitation applies in POA as well as in the Windows authentication window (Windows logon, locked desktop, standby or hibernate resume, screen saver, etc.). After 5 unsuccessful attempts, your computer will instantly become locked out and you will be stuck in POA mode. Then, the only way to unlock the system and use it again will be to contact the E-TAC for doing a challenge-response logon. This procedure is the same as recovering a lost password (section 3.3).

### **2.3 Changes to the Windows environment**

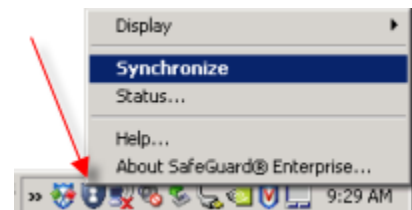
---

When you look in “**My Computer**”, you can see the **green key** icon that tells you the hard drive is **encrypted and readable** by the currently logged user. A **yellow key** means the drive **is being encrypted or decrypted** and a **red key** correspond to a drive or partition that **could not be read** by the currently logged user.



If you **right-click** on the encrypted drive and **select properties**, you see this new “**Encryption**” tab. It illustrates the keys that were used to encrypt the drive.

The workstation must synchronize periodically to the SGN server in order to receive policy updates and exchange key and certificate information. This is done using an agent that installs to Windows along the installation of the product on a workstation. This agent puts an icon in the system tray, which takes the shape of a purple shield with a keyhole. If you need to force synchronization with the server, right-click on this icon and click on “**Synchronize**”.



Note that the Safeguard Enterprise system is available via CGINet, SERA-Full, the Internet and RNAS corporate services profiles and the Internet.



---

### 3 FREQUENTLY ASKED QUESTIONS

---

This section presents answers to frequently asked questions.

#### 3.1 Is there any risk of losing my data?

---

Like any computer system, a hardware failure may happen and this failure may damage the data of the hard disk partially or completely. In many situations, defective drives can be salvaged by desktop support professionals, but in rare cases, data cannot be restored and is lost permanently. It is strongly recommended to perform regular backups of the files and folders, in case the hard disk becomes unrecoverable.

Because of its nature, data encryption may reduce the chances to salvage data from a broken hard disk. Therefore, you should keep this in mind and take backups regularly. You should work from the network as much as possible, on file servers with daily backups.

More importantly, your hard disk is encrypted in order to protect your data from unauthorized people. Therefore, **keep your backup media in a safe place**, and not on your desktop or in your laptop carrying case.

#### 3.2 How do I change my logon password?

---

If you wish to **change your network password**, the recommended process would be to check “Change password at next logon” from POA options at start up. It will then bring you to the Windows logon prompt and the system will ask for your current and new password you would like to set.

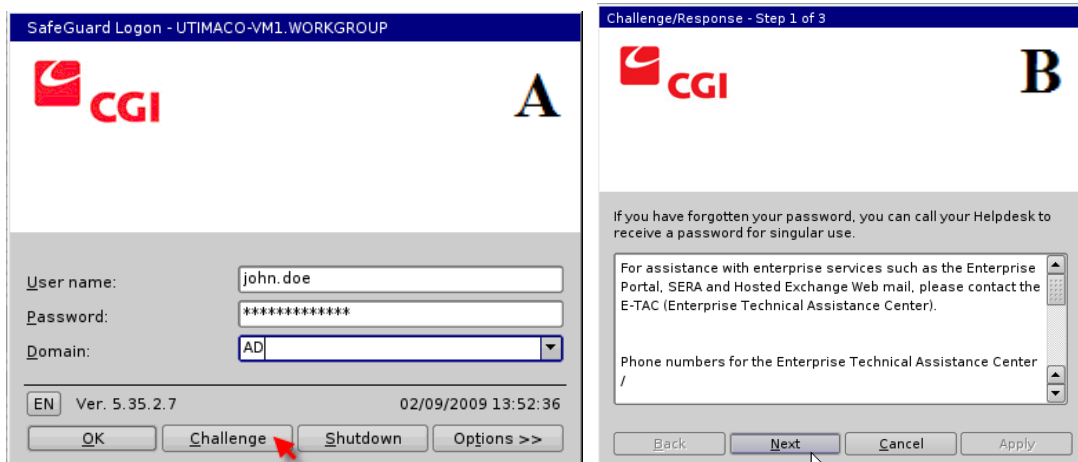
When the new password has been entered, **the system will update the information automatically**.

**Important note:** If you own two laptops and you have changed your password on one of them, you must remember that the second laptop will not be updated and you will have to enter your old password at the POA to get access to the PC. Here is the proper procedure to make sure your second laptop gets updated correctly.

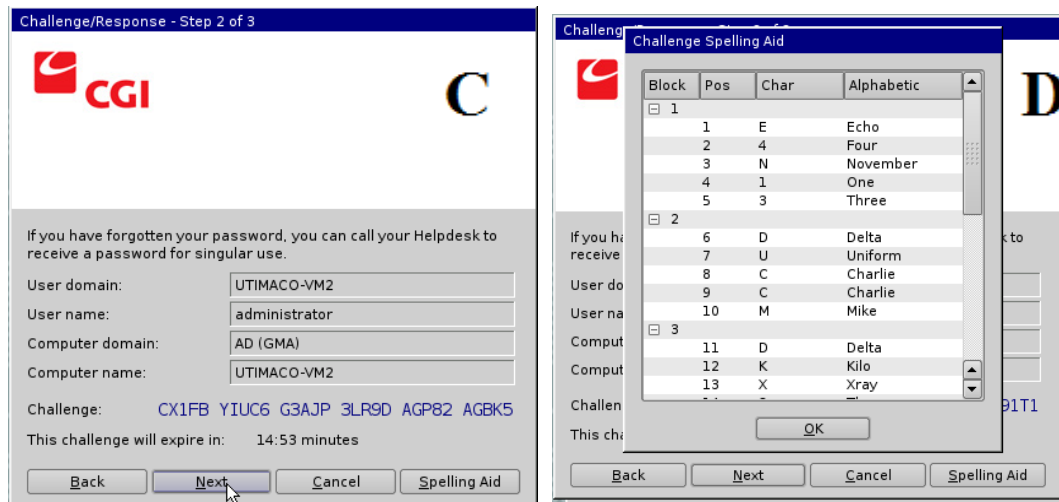
- 1- Make sure the laptop is connected to the network.
- 2- Enter your old password at POA. If you do not remember your old password, you will have to contact the E-TAC and perform a challenge-response.
- 3- The system will stop you at the Windows login screen (If not, you might not be connected to the network correctly)
- 4- You can now enter your current network password and the system will now be up to date.

### 3.3 How do I recover a forgotten logon password?

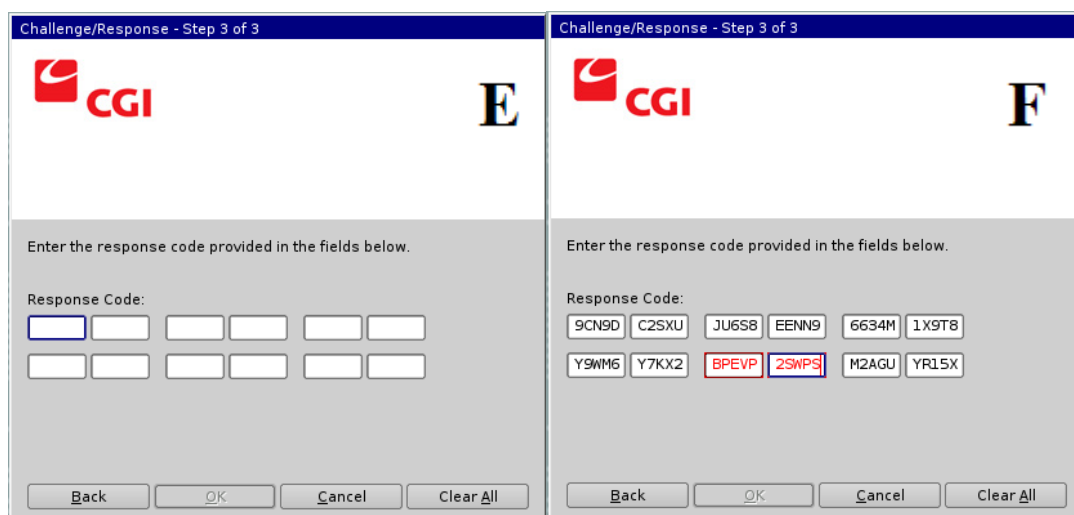
1. Contact the E-TAC assistance center to initiate the **challenge-response mode**.
2. **Enter your Username and click on the Challenge button** on the POA screen (image A).
3. Refer to this message window to know your local **Enterprise Technical Assistance Center** contact number (image B)
4. Note that you will have **15 minutes** to complete the challenge procedure.



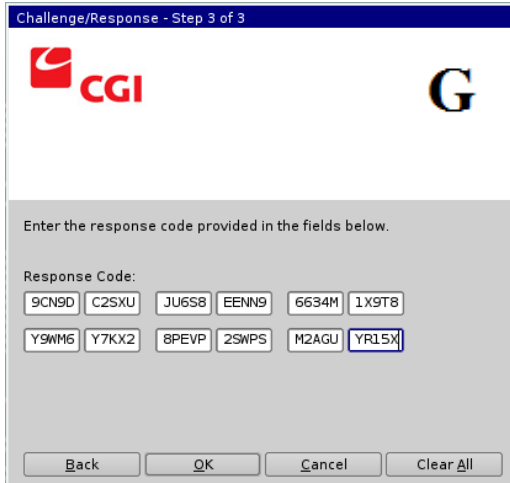
- Dictate the **30-character alphanumeric challenge code** that appears in blue at the bottom of the screen (image C). To ease oral communication of the code, **click on the Spelling Aid** button, and **dictate the code** using phonetic alphabet (image D).



- The helpdesk agent will now enter your code in his system that will generate another code. He will inform you that after ending the communication with you, he will leave the response code on your CGI voicemail as a security measure.
- You will have to **type in the response code** in the twelve text fields (image E below). If you made any mistake in typing, the fields to verify will be displayed in red (image F below).



If the code is typed correctly, all fields will appear in black, and the OK button will be clickable (image G below). If you cannot enter the correct code or the agent's message was not recorded properly on your voicemail, you will have to start over from step 1.



8. You can now **click OK**, and the system will boot normally and start your Windows session. **Contact your local TAC** and ask for a password reset. The local TAC will give you a temporary password. **Do not reboot**, or else you will have to start the challenge-response again.
9. Once the local TAC gives you a temporary password, change it while still logged in Windows by following section 3.2.
10. When the new password has been set, **the system will update the information automatically** but if you want **to manually push those changes**, right-click the **SGN system tray icon** and choose **“Synchronize”** as described in section 2.3 of this document.

### **3.4 How to give access to my computer to another user?**

---

This section explains how to give access to your computer to another user (for example a colleague that will replace you and use your laptop for some time). **Never tell your password to another user, as it constitutes a major security breach and violates the CGI corporate security policy.**

As a premise, make sure the user you want to give access to your computer was already authorized to logon to Windows on your workstation prior to the installation of Safeguard. If this is not the case, you must request this to your local IT support.

Assuming the user has access to your machine at the Windows level, you must grant him access to your machine at the POA level. The following steps must be done once, and the user will be able to logon using his credentials afterwards.

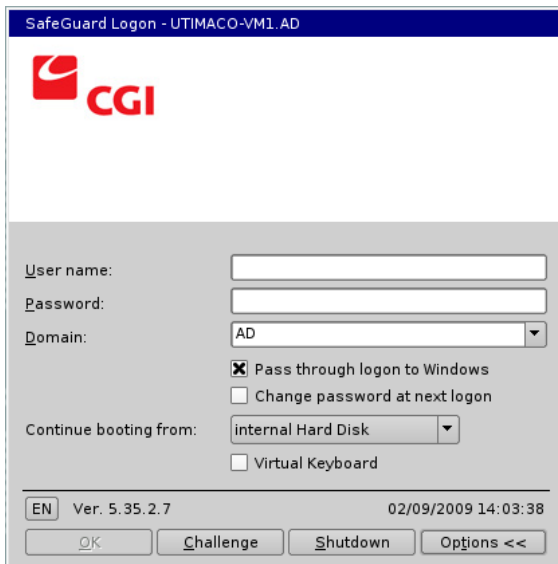
In the POA, press the **“Options”** button and **remove the checkmark** from **“Pass through logon to Windows”**. Enter your credentials as you do for normal logon. Windows will start and bring the **Windows logon screen**. Do not enter your credentials here. Instead, have the other user enter his username and password. After logging in at the first time, that user will be able to log in to the system (including POA) using **his own credentials**, and use the computer under his local user profile.

**Note:** If the procedure does not seem to work, it is possible that, for some reason, you are not identified on your system as the “owner”. In that case, please contact your local technical support center to get the assistance you require.

### 3.5 What are all those advanced options on the POA screen?

---

At the POA screen, there is a few other options available and we will cover them all in this section.



The screenshot shows the 'SafeGuard Logon - UTIMACO-VM1.AD' window. It features the CGI logo at the top left. Below the logo, there are input fields for 'User name:', 'Password:', and 'Domain:' (set to 'AD'). There are two checkboxes: 'Pass through logon to Windows' (checked) and 'Change password at next logon' (unchecked). A 'Continue booting from:' dropdown menu is set to 'internal Hard Disk', and a 'Virtual Keyboard' checkbox is unchecked. At the bottom, there is a status bar with 'EN', 'Ver. 5.35.2.7', and the date/time '02/09/2009 14:03:38'. Four buttons are visible: 'OK', 'Challenge', 'Shutdown', and 'Options <<'.

- **The Challenge button:** If you need to log in that computer but do not know/remember the password, you can call your IT helpdesk to initiate a challenge-response to gain access to that computer.

The process is quite simple, you give the Challenge code to the helpdesk agent and then you press next. The agent will now enter that code in his system and give you another code to enter on your system for then being able to log in. There is a time limit for this whole process and it is 15 minutes.

- **The Options button:** If you click on “Options”, you will have a few other choices.
  - **Pass through logon to Windows:** If enabled (it is by default), it will use the credentials you enter in the POA to login to Windows automatically.
  - **Change password at next logon:** Makes it possible for you to manually trigger a password change the next time you log into Windows.
  - **Continue booting from:** Gives you the option to boot from another device after logging to the POA.

- **Virtual Keyboard:** At the POA a user may show/hide a virtual keyboard on the screen and click the on-screen keys to enter credentials etc.

### **3.6 How do I change my keyboard layout in the POA?**

---

The POA keyboard layout reflects the one set in Windows. To change it, logon in Windows, select **Start > Control Panel > Regional and Language Options > Advanced**. In the **Regional Options** tab, select the required language. In the **Advanced** tab activate option **Apply all settings to the current user account and to the default user profile** under **Default user account settings**. Confirm your settings by clicking **OK**. The POA remembers the keyboard layout used for the last successful logon and automatically enables it for the next logon.

If for any reason the keyboard layout gets changed unexpectedly (e.g. an unwanted or accidental change in Windows that replicates to POA), and you are unable to enter your password correctly, click on **“Options”** in POA and check the **“Virtual Keyboard”** box. You may click the virtual keys to aid finding the characters that compose your password. Once in Windows, you may change back the keyboard layout to your convenience.

### **3.7 Will the files I send through e-mail or put on an external media be encrypted?**

---

The laptop encryption solution does full disk encryption. Only the hard disk in your computer will be encrypted. Once you logon to POA, your data is unlocked for the duration of your session. Thus, as long as you are logged in, your files and folders behave like they are not encrypted at all.

In other words, when you send emails with attached files, those files won't be encrypted unless you use an email encryption solution (which is not part of Safeguard). Files you put on a CD, USB storage drive, SD card, backup tape or any other external media, will be stored without encryption, so you should keep them in a secure place. If you share a drive or folder on the network, people who are authorized to access data located in the shares will have access even if they don't have access physically to your workstation. Similarly, files you put on network share will not be encrypted.

Only the files that reside in your hard drive are encrypted. Once they get out, they lose their encryption. Keep that in mind while sharing files.