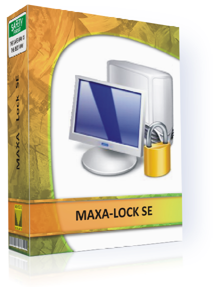
MAXA-LOCK-SE

Document Revision EN V 2.3a

True Security For Your Data



Preamble

Throughout history, security and self-protection has always been, among everyone's basic requirements and rights. What has changed is society itself - culturally, politically, legally and technically. The vulnerability of today's IT systems to modern attack methods has several similarities to the Cold War with both competing offensive and defensive technologies.

Why Data Security?

It has never been more important to protect confidential information & electronic data – both commercial and private. In these times of global communications and worldwide networking sniffing out electronically-stored data by hackers, crackers, co-workers, unauthorised personnel and other such groups has become relatively easy.

Industrial espionage has been around in the business world for a long time, and has caused billions of dollars worth of damage. Even the service sector, which provides services to the normal citizen, gives cause for concern in security matters. Things have not stood still in the personal data area. ‘Social Engineering’ methods alone have increased tremendously.

The trade in illegally-obtained data, as a result of insecure data management, has become a highly-profitable industry. The combination of legally-obtained material with that obtained illegally can, when misused, cause serious damage.

Digital technology theoretically permits the capture, transmission and distribution of any image or audio file in an instant. Governments in the industrialised world have caused enormous amounts of data to be accumulated, such that their citizens become numbers. In addition the current or planned number of on-line monitoring of PC users by various governmental bodies is finally bringing about a ‘Big Brother’ situation.

Well-known examples are:

- Echelon (world-wide system)
- Carnivore (FBI)
- “EU-Trojan”
- Security monitoring cameras
- Criminal investigations
- Illegal pooling of data from multiple databases
- RFID (*Identity cards, passports, pricing labels*)
- Points records for traffic offences

Similarly, in the commercial area, enormous quantities of data are captured and stored daily. In many cases, governments can obtain, or legally demand, access to:

- RFID (*price labels*)
- Credit data
- Loyalty cards
- Bank or credit cards
- Voice and internet providers
- Health bodies (*doctors, health authorities, health insurance companies*)
- Lawyers, tax accountants (*e.g. data trails or exchanges with corresponding lawyers*)

How has this happened?

Attackers have not only refined their methods, they have also become far more efficient. Since operating systems do not pay sufficient attention to these applications, these security gaps must be closed using third-party systems. It is also vital to educate & encourage users, and to provide them with every possible assistance.

The very groups or individuals who bear the heaviest legal responsibilities for the care and confidentiality of data have the least awareness. This includes:

- Lack of security consciousness
- Ignorance of legal responsibilities
- Inactivity by those in positions of responsibility

Anyone who believes that their data is sufficiently protected by Windows encryption, stored on hard disk (*e.g. Windows NTFS*), has been misled. These days there is no problem in accessing electromagnetic radiation from a PC monitor. This can be exploited from a short distance away, e.g. from a parked car, and the resulting data collected and reconstituted. Unauthorised access is made much easier when a user leaves their workstation unattended, without doing enough to block access. A lost or stolen laptop can, if unprotected, be an open book.

Networking PCs means a much greater danger of illegal access to data. The type of networking is actually irrelevant - every data transfer between sender and receiver means that there will be security weaknesses.

The size of the danger posed to data, along with its administration, means the only possibility is for users to secure their data themselves.

What can be done?

In addition to being security-aware, users need to keep up-to-date and use suitable security tools such as those offered by MAXA.

Who should use MAXA-Lock-SE?

Anyone who seriously wishes to protect sensitive data or any individual who from time to time uses the internet and wishes to protect their files from online monitoring.

Who definitely needs MAXA-Lock-SE?

Those in positions of responsibility, and professions where confidentiality is a legal requirement.

Professionals, who are required, by law, to protect the data and confidentiality of their clients and/or customers:

- pharmacists
- doctors
- practicing psychologists
- notaries
- solicitors/attorneys
- tax accountants
- auditors

If media reports are to be believed, there is a real lack of awareness of the changing security situation amongst these professional groups.

Doctors are particularly prominent here ('Self-check' for General Practitioners), closely followed by lawyers' chambers.

Consulting practitioners

- religious matters
- psychosocial consultants

Public positions

- e-Government

Commercial sectors:

- Computer centres
- Associations & societies
- Federations
- Banks
- Insurance companies
- Insurance agents
- Address brokers
- Marketing and market-research companies
- Call-centres
- Telecom providers
- Service providers

MAXA-Lock-SE:

One of the biggest threats occurs when the work-station is left unattended, or is not switched off. It makes sense to leave a PC running, since this extends the useful life by reducing power-ons and power-offs (*which in turn reduces temperature variations in the warm-up and cooling phases*). Let's take a practical example, and consider the following recommendation:

Many Data Security Laws stipulate that data processing systems holding personal data should be protected from unauthorised access. Additionally, personal data should be protected from unauthorised access or data-processing.

That means that access to unattended PCs should be blocked. Clearly, if this risk is not catered for there is an obvious security threat. It is now recognised that the various screensaver solutions are no longer up to the task, since they can easily be bypassed by a hacker. We need to use an external solution instead.

Our software-house has been successfully involved in the security arena for many years. Even today, applications such as MAXA-Crypt-SE are seen as 'uncrackable'. For the wider application market we have now concentrated on some additional focal points, e.g.:

- Automatic access control
- Soft lock
- Intuitive user guidance
- Internet-integration
- Screen-saver emulation
- Info-screen
- Multi-media support
- Skype-integration (*Pro version only*)
- Multilingual (*German, English, Spanish*)

The end-result is a desktop-security software known as MAXA-Lock-SE, the first to offer multi-media capabilities and also Skype-integration.

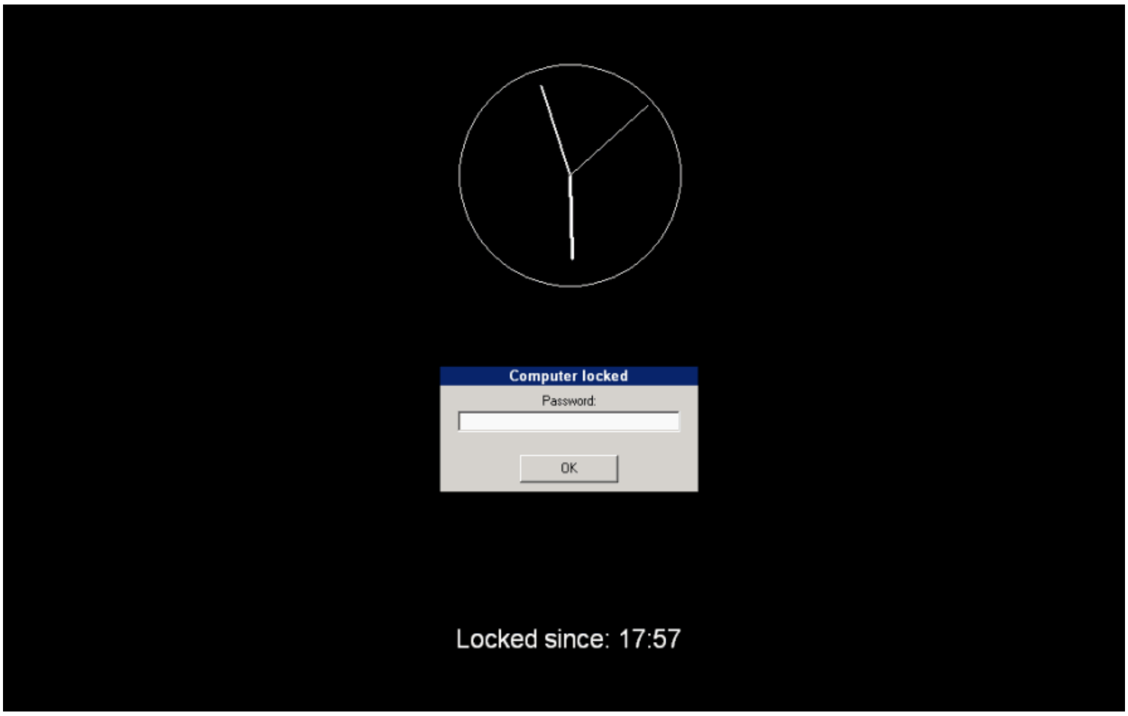
What is MAXA-Lock?

MAXA-Lock is a Windows software application which helps users to conform to their security requirements by reliably protecting their unattended systems, without them having to be switched off.

What can MAXA-Lock-SE do?

The software obscures the monitor temporarily, limits the functionality of input devices such as the mouse or keyboard, such that unauthorised personnel cannot view or access the contents of Windows PC. Naturally this also handles unauthorised remote control systems, e.g. from an Internet-café. If a user leaves his PC and forgets to switch on the protection system, a Security Sensor Timer would activate it after a selected time period.

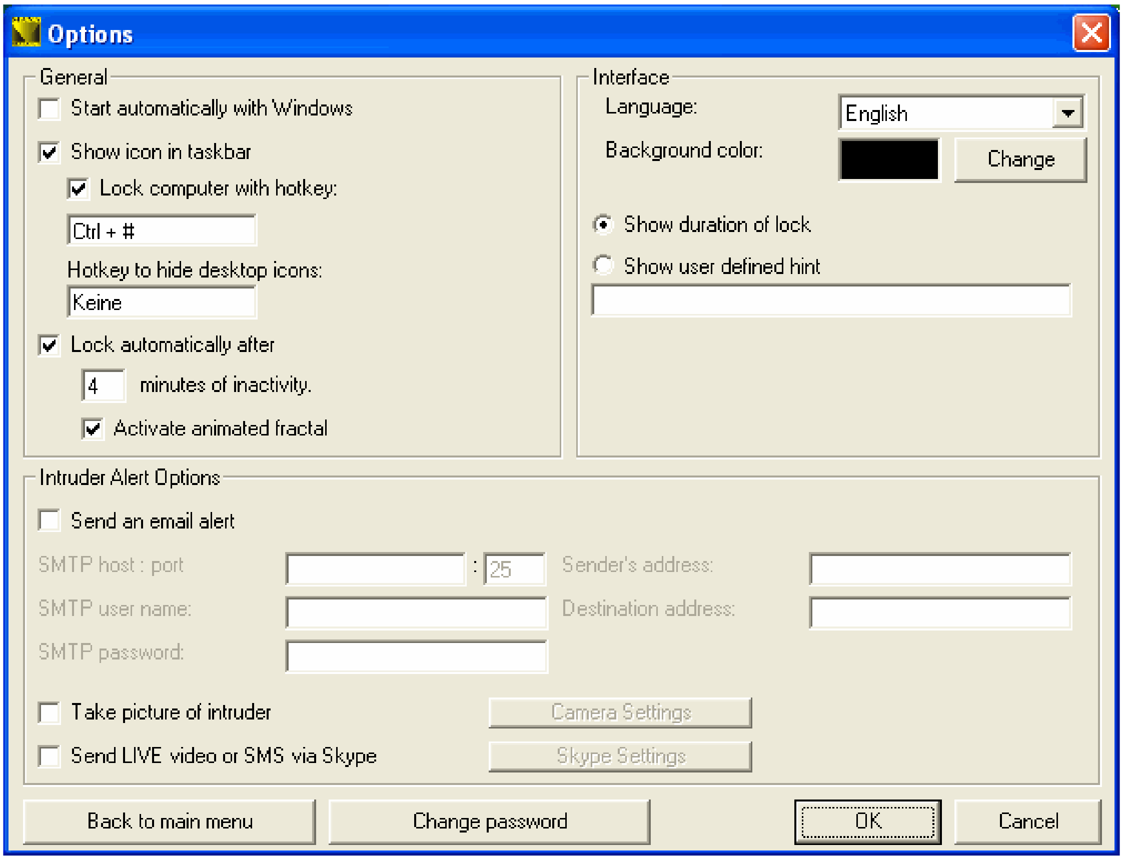
Shows the screen, when MAXA-LOCK-SE is active.



Locked since: 17:57

Anyone who works for long periods in front of a PC screen needs to take breaks. Both physical and mental relaxation are important, to relax the mind and improve alertness. We provide optical support by implementing a fractal screen-generator. Complex mathematical calculations generate an infinite sequence of flowing, soothing geometric patterns. The mix of structure, colour and time phases coordinates the observer's relaxation. Pressing a key or moving the mouse switches the screen back to the security display. The integral Anti-Icon mode causes desktop icons to temporarily disappear from view. Airline travellers can hide from their neighbours which systems are installed on their PC. If for some reason the PC has to be closed down quickly, this can be done via an icon in the MAXA-Toolbar.

Option Menu (Skype support in Pro version only)



Options

General

☐ Start automatically with Windows

☑ Show icon in taskbar

☑ Lock computer with hotkey:

Ctrl + #

Hotkey to hide desktop icons:

Keine

☑ Lock automatically after

4 minutes of inactivity.

☑ Activate animated fractal

Interface

Language: English

Background color: ■

● Show duration of lock

○ Show user defined hint

Intruder Alert Options

☐ Send an email alert

SMTP host : port : 25

Sender's address:

SMTP user name:

Destination address:

SMTP password:

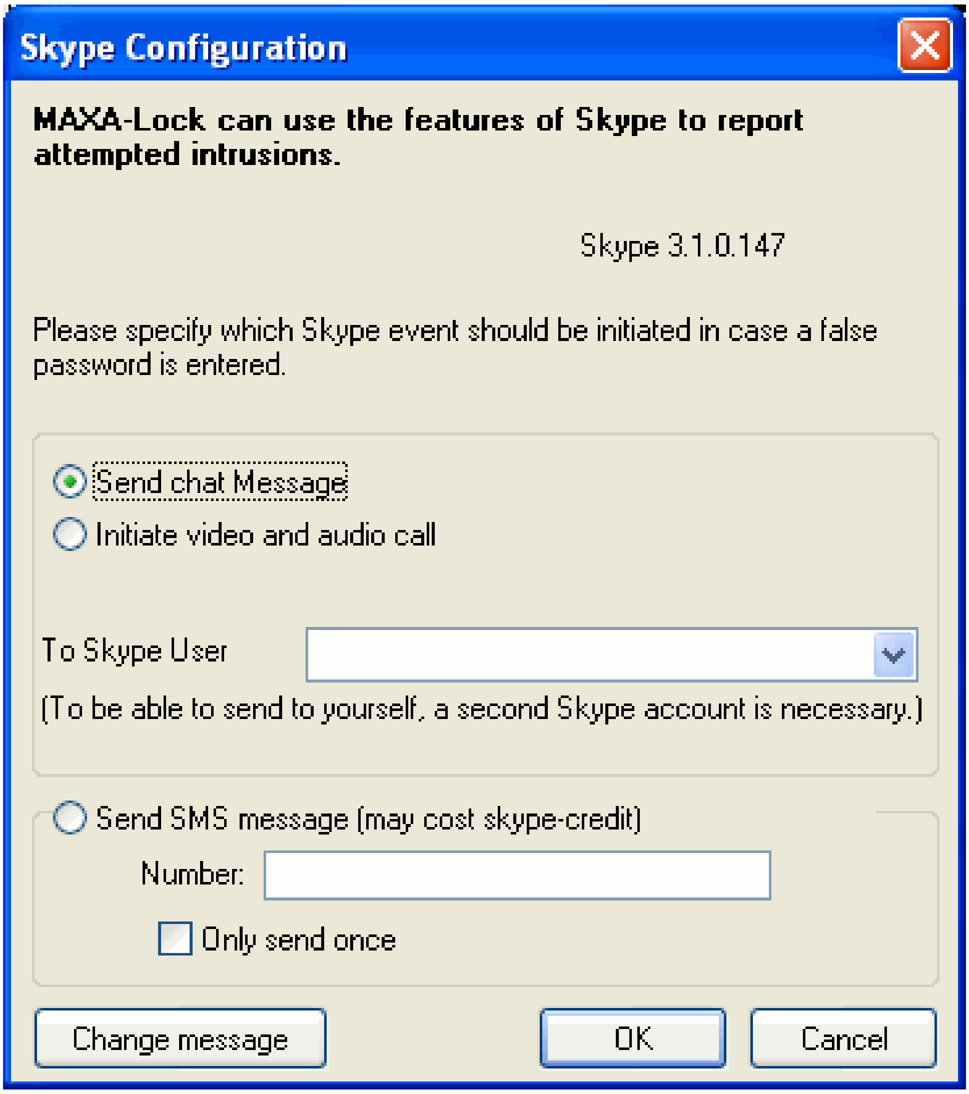
☐ Take picture of intruder

☐ Send LIVE video or SMS via Skype

This is the main Option menu for MAXA Lock SE. General options are at the top of the dialog box, including Starting automatically with Windows, Hot Keys, Activate/Deactivate Fractal images and language.

The bottom half of the dialog deals with options for relaying intruder information. From here, you can setup email and/or, if you have a webcam or IP camera near or on the computer, you can setup to send pictures via SMS or Skyp or even record live video of the intruder.

Setup for Skype (Pro version only)



Skype Configuration

MAXA-Lock can use the features of Skype to report attempted intrusions.

Skype 3.1.0.147

Please specify which Skype event should be initiated in case a false password is entered.

● Send chat Message

○ Initiate video and audio call

To Skype User

(To be able to send to yourself, a second Skype account is necessary.)

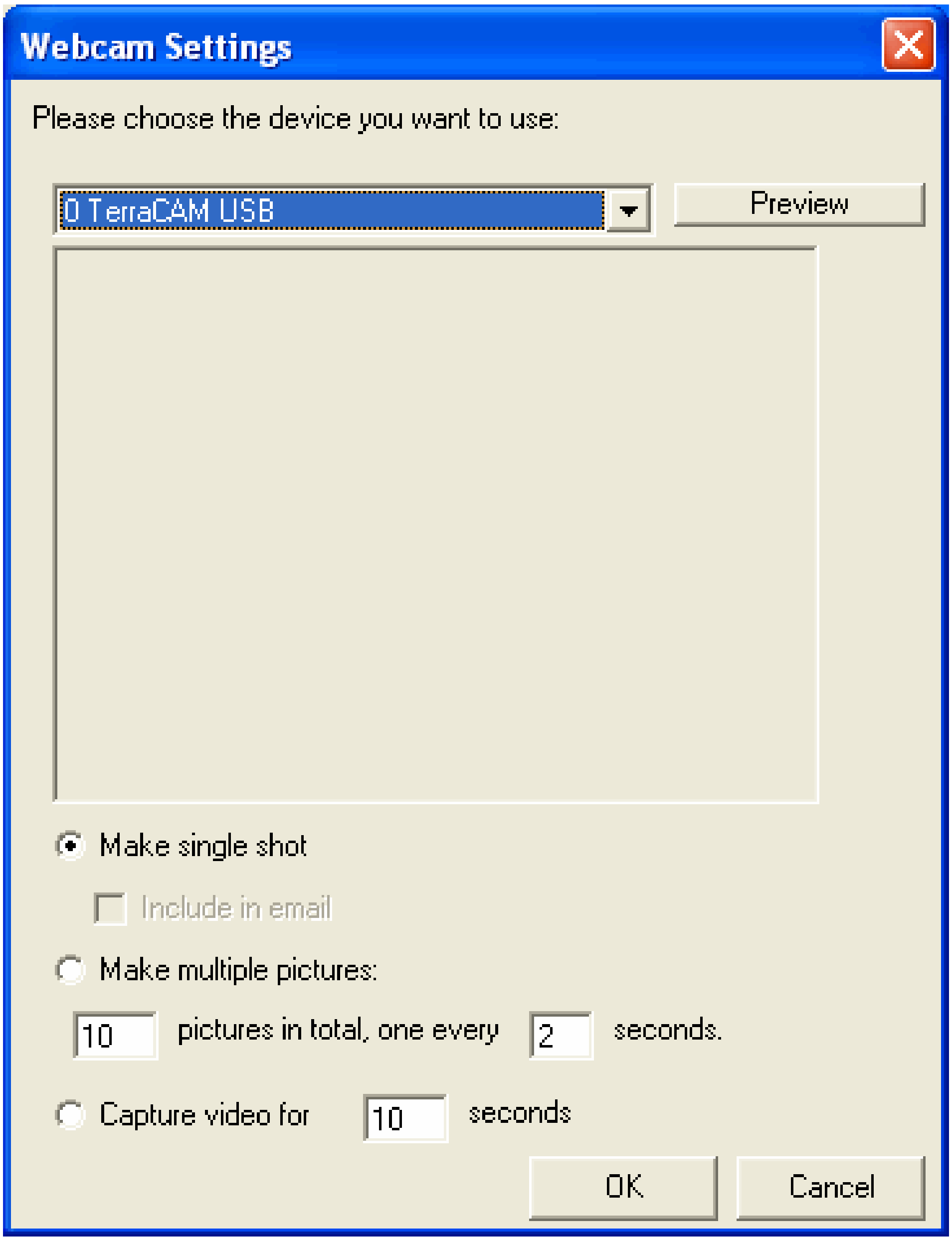
○ Send SMS message (may cost skype-credit)

Number:

□ Only send once

Use this menu to select what Skype options you want to utilize if an intruder is detected.

Cam Setup



Please choose the device you want to use:

0 TerraCAM USB

● Make single shot

□ Include in email

○ Make multiple pictures:

10 pictures in total, one every 2 seconds.

○ Capture video for 10 seconds

Use this option to determine how to take pictures (*webcam or IP cam required*). You can take a single shot and email it to someone or you can take multiple pictures or even capture video.

How does MAXA-Lock handle attacks?

If an incorrect pass-phrase is put it, this triggers an alarm procedure to produce various warning-levels. Where practical, warning-levels can be combined.

Mail Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If multiple PCs are blocked, the PC names are used to differentiate.

Picture Mail Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If a Web-camera or IP-camera is connected, the image captured will also be forwarded. If multiple PCs are blocked, the PC names are used to differentiate.

Video Mode:

Each wrong pass-phrase is recorded and forwarded by email to a specified address. If a Web-camera or IP-camera is connected, the individual image is captured and a sequence of images or a complete video will be stored: these can be displayed locally after unlocking the workstation.

Skype Mode (Pro version only):

Each wrong pass-phrase is recorded and forwarded via Skype to a specified Skype address as a chat message. If a Web-camera or IP-camera is connected then everything that the camera captures will be forwarded live.

If you concealed the camera somewhere in your room then this will not be obvious to the person being monitored. Anyone with mobile Skype access will be able to utilise this service in both ways. Alternatively the information can be sent via SMS.

Can you be confident in MAXA-Lock-SE?

No security measure is 100% certain secure against attack! However, in practice the effort required can exceed what is practical (physically, thermo-dynamically, etc.) In other words, the effort required bears no relation to the chances of success.

In MAXA-Lock-SE, in addition to the professional software methods employed, we also put in various blocks and counters to the various tricks and tactics used by hackers and crackers. So in order to carry out a practical attack, more and more time will be required. As this goes on, the alarm responses are being triggered and evidence is being gathered. The attacker will soon decide to break off his activities, in order not to compromise himself further.

What versions of MAXA-Lock-SE are there?

There is a standard version, free-of-charge for registered private users: note that this version (*MAXA-Lock-SE-Standard*) has no Skype support. Updates for this version are also free, as long as the user is registered with a valid email address (*also free-of-charge*).

MAXA-Lock-SE *Pro*. The Pro Version supports Skype (*see:* www.skype.com *please*) is supplied as a licensed package for two installations. This licence is linked to a single user, and is not transferable. MAXA-Lock Pro is already built in **MAXA-Crypt-SE** and **MAXA-Security-Tools.**

Minimum hardware and software requirements for MAXA-Lock-SE.

Hardware:	Pentium II, 266MHz, VGA, keyboard & mouse (*or equivalent*)
Software:	Windows 98 / 98 SE /ME / 2000 / XP /Vista or equivalent.

Note:

- Internet access required to register the product on installation and to receive updates.
- Errors & Omissions Excepted
- This paper reflects the technical situation as at January 2008
- MAXA and the text and image references are registered trademarks of MAXA Research International, Inc.
- Any other trademarks mentioned are the property of the registered owner.

➢ **END**