USER GUIDE

Installing encryption on a PC *(MAC SEE PAGE 7)*

1   BEFORE YOU INSTALL – TWO IMPORTANT CHECKS

Windows 8 and 10 has a different way of handling user accounts from Windows 7, so please read the following before installing.

#1. **You need to be a local user and HAVE A PASSWORD.** In Windows 8 and 10, there are two different types of user accounts – a Local User account OR a Microsoft Account. Microsoft wants you to use their “Microsoft Account” as standard. This is an Internet account and will not work for the encryption installation. Your machine will not be connected to Internet when you authenticate to the encryption – if your machine was connected to Internet at that stage, there would be no protection for your data.

For the installation to be successful, you have to have the local account enabled during the installation.

To check the current account status, please follow these steps:

- Go to settings (the cog sign).
- In Windows 8, choose “Change PC settings” at the bottom of the screen.
- Click on “Accounts”
- Under “Your account” and your login name, you will be able to see if you are logged in under a “Local account” or a “Microsoft account”.
- If the grey button says “Switch to a local account”, please click on it and follow the instructions. Please note that you need to choose a strong password (rules below).
- If the grey button says “Switch to a Microsoft account”, you are OK. However, please note that you need to have a strong password.
#2. You need admin rights on your machine. Normally you already have this, but computers that belong to larger organizations may have reduced administration rights for you as a user. If this is the case, you may have to contact the IT department in your organization and have the installation run under an administrator’s account.

If you are using or upgrading to Windows 10, you will need to have Windows 10 “Anniversary update (aka “Redstone”) before you install.

We recommend making a backup of your data before installing any software.

**Strong Password rules for AlertSec clients.**

- **Length:** 6 digits minimum
- **Content:** Upper AND lower case AND number(s)
  - Update your password by clicking on the “Change your password” button. Picture passwords are not supported.
- **Max logon attempts:** Max 3 attempts before temporary lockout and forced reboot, then another 2 attempts before lockout.

2 INSTALLATION

In the installation email you are sent from the system (your coordinator), there is a web link included. Click on that and follow the instructions.

The installation is done in two steps.

#1. After answering three security questions a Device Agent installs and connects to the AlertSec software server. Once that is done, it will download the software packages and the relevant policy settings for your installation.

Installation time varies depending on the Internet connection you have. You will also need to restart the machine twice before everything is installed. **You can carry on working as normal during the download and installation and you will always have a chance to save any work before the restarts and/or postpone the installation.**
Depending on your OS and your computer configuration, the installation process will look slightly different, but you will need to confirm that you are happy to install the software.

To monitor the installation progress, click on the padlock and “Display Overview” in the lower right corner of the screen.

*Before the computer receives the policy a security warning may be shown - this is normal. If Anti-malware is included in your policy, it will receive the first update within 2 hours from installation. Updates can be forced by clicking on “Update Now”.*
The Full Disk Encryption will also collect your Windows user credentials. This is called “User Acquisition”.

As soon as the system has collected your user credentials and sent the necessary information to the AlertSec server, you will be asked to re-boot again.

Login with your current Windows credentials – these will still be used onwards.

The machine will now start the encryption. This is a low-priority process so you can use the machine as normal. You can also close the machine down at any time, even if the encryption hasn’t finished. It will resume the encryption as soon as you re-boot next time.

**3 COMMON INSTALLATION ISSUES THAT YOU CAN SOLVE YOURSELF.**

**#1 installation is stuck on “User Acquisition”**

This is the most common issue you can come across and it is related to either:

#1 You have not a user account with a password – if there isn’t a password or you have several users on your computer, the User Acquisition may not work and the encryption will not start. Please add a password to your account, then log out and log in again with your new credentials. Make sure you chosen a strong password.

#2 You are not using a “Local Account” - see 1.1 above.

**#2 Microsoft says it is unsecure software**

Depending on your operating system and settings, you may be prompted NOT to install this software. Choose advanced and “allow anyway”.

**#3 It doesn’t seem to start the encryption**

The encryption starts after a successful “user acquisition”, “set up protection”, and the subsequent reboot. The encryption will only run while the machine is on, but it is safe to turn it off during this process as it will continue as soon as you boot up again. It is good to leave it on over night after the installation to let it finish the encryption. You can follow the progress by clicking on the Check Point padlock in the tray.
#4 I have forgotten my password

No problem. Should you lose or forget your password, the AlertSec Helpdesk can assist you. The service is open 24/7 and a reset can ONLY be done over the phone, NOT email. You do not have to be online to receive help, but you do need to be able to answer the security questions you set up during installation.

The numbers to call are:
- US TOLL-FREE: +1 (888) 473-7034
- UK: +44 1962 738336
- Sweden: +46 8 525 00 972
- Rest of the world: +44 1962 738336

#5 Can I resize my partitions?

NO. Never use any disk partition editing software when the Full Disk Encryption is installed on the machine. If you need to resize a partition, remove AlertSec Full Disk Encryption completely, and then resize the partition.

#6 How do I uninstall

If you wish to uninstall, you have to contact your coordinator who is the only one that can authorize a decryption of your computer. He will have an uninstall password available – see coordinator’s guide.
INITIAL INSTALLATION - MAC

BEFORE YOU INSTALL – 2 IMPORTANT CHECKS

#1. You need local admin rights on your machine. Normally you already have this, but computers that belong to larger organizations may have reduced administration rights for you as a user. If this is the case, you will have to contact the IT department in your organization and have the installation run under a different user account.

#2. You need a Mac account with a strong password. If you haven’t, please click on the “apple” then “system preferences” and “accounts”. From here you can change or add a password to your account. Log out and log in again with your new password before installation to make sure it is implemented.

We recommend making a backup of your data before installing any software.

Please check the system requirements on the AlertSec website.

LIMITATIONS

Direct upgrade from earlier OS versions is not supported. Instead you must Uninstall AlertSec Encryption, upgrade your OS and install AlertSec Encryption again.

Hardware limitations

- Encryption of new disks added to the system after the initial AlertSec installation is not supported. You must uninstall and then reinstall AlertSec to have these encrypted as well.

Software limitations

- Apple RAID driver is not supported.
- Boot Camp Assistant cannot be used to install Boot Camp multi-boot functionality after AlertSec has been installed.
- Imaging: You cannot generate a generic image with AlertSec Encryption pre-installed.
About File Systems/Volumes

- AlertSec Encryption supports the encryption of only one disk.
- To install AlertSec Encryption, the disk must be partitioned using the GUID Partition Table (GPT) scheme. Use the Disk Utility tool to see which partition scheme is used on a disk.
- You can select a maximum of thirty-two volumes to be protected by AlertSec Encryption.
- Never use any disk partition editing software with AlertSec Encryption installed on the computer. If you need to resize a partition, remove AlertSec Encryption completely first and then resize the partition.
- Do not use disk utilities to change file systems or resize any volumes on the hard disk if AlertSec is installed. Doing so may lead to an unusable system.
- USB memory sticks to be used as recovery media must be in Mac OS Extended Format (HFS+ format). Use the Disk Utility to reformat non-HFS formatted USB memory sticks.

Strong Password rules for AlertSec clients

| Length: | 6 digits minimum |
| Content: | Upper AND lower case AND number(s) |
| Max logon attempts: | Max 3 attempts before temporary lockout and forced reboot, then another 2 attempts before lockout. |

INSTALLATION

You will receive an installation email from your coordinator, please click on the included web link, fill in your personal authentication questions and download the relevant software version.

The installation is done in the same fashion as any other software installations. You will need to confirm that the software can be installed.
Once the code is installed, you will need to log out and the log in to the machine so the software can pick up your user name and password. Please make sure you have chosen a strong password before doing this.

Installation time varies depending on how large your hard disk is as the encryption time is directly proportional to the size of the disk.

**LOGIN**

Once the software is installed and you have rebooted your machine, you will be asked to login at the pre-boot screen. Use the same user name and password as you normally use on your Mac.
CHECK ON PROGRESS/ ENCRYPTION SETTINGS

You can check on the progress of the encryption or the settings if you click on the padlock in the heading on your screen and choose "Display Overview".

<table>
<thead>
<tr>
<th>Help</th>
<th>Wed 24</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display Overview</td>
<td></td>
</tr>
<tr>
<td>Quit</td>
<td></td>
</tr>
</tbody>
</table>

CHANGING YOUR PASSWORD

We recommend that you change the password in your Mac OS, rather than in the pre-boot screen. However, if you are prompted to change your password you will also need to change it in the OS.

I HAVE FORGOTTEN MY PASSWORD

No problem. Should you lose or forget your password, the AlertSec Helpdesk can assist you. The service is open 24/7 and a reset can ONLY be done over the phone, NOT email. You do not have to be online to receive help, but you do need to be able to answer the security questions you set up during installation.

The numbers to call are:
US TOLL-FREE   +1  888 473 7034
UK:             +44 1962 738336
Sweden:         +46 8 525 00 972
Rest of the world: +44 1962 738336

HOW TO UNINSTALL

If you wish to uninstall, you have to contact your coordinator who is the only one that can authorize a decryption of your computer.