ScoMIS Encryption Service

Primary School Deployment Guide

Introduction

This guide explains how to implement the ScoMIS Encryption Service for a primary school. ScoMIS has made the installation process very easy through development of a wizard based installation process. We recommend that in a primary school the software should be installed onto the laptop by the end user (normally the teacher).

Audience

We recommend the school's person responsible for ICT implements the steps in this deployment guide and gradually releases the software to their users. If you have a full time technician or network manager you should also take a look at the deployment guide prepared for secondary schools to see if that model of implementation suits your school better.

Contents

an excellent authority

★★★★

audit commission

Chapter 1 – Implementation Summary

Summary of deployment process – covered in detail later in the guide

1. School places their order online at http://www.scomis.org/go/encryption
2. ScoMIS email school links to the *Deployment Guide* and release the software for download.
3. School download the software onto their network ready to be installed onto the Laptops

   Note: We will be carrying out a phased rollout during the initial launch of the service to maintain high levels of service on our Service Desk. This means there will be a delay between the time you receive the documentation and the installation key

4. ScoMIS send the school their installation key via email
5. Installations can begin in school

Summary of installation process – covered in detail in the installation guide

1. School give the user the installation guide, network location of the encryption software setup, installation key and any advice relevant on backing up
2. User makes sure they have a backup on the school network or other physical device of all data on their laptop
3. User carries out a CHKDSK (scan disk) to make sure the laptop hard drive is mechanically good
4. User installs the Encryption software
5. During installation the user is given a new username and chooses a strong password
6. After installation the hard drive is automatically encrypted – this is transparent to the end user and aside from them having a new logon username and password doesn't change the way they use the laptop or Windows in any way.

Chapter 2 – Implications of Encryption

Once encryption has been installed and implemented onto your laptops there maybe a number of changes to the way you use laptops in school. We have tried to identify these below:

- **Unique usernames** – every one of your users who has access to the encrypted laptops will be setup with a unique username.
- **Controlled Access** – only users which you assign to the device during installation or later through our maintenance utility will be able to log on. However you can add many users or you may choose to allow all teachers to log onto all laptops for example.
- **Strong Passwords** – each user will have a strong password with a minimum of 8 characters that is changed every 42 days. Users must never divulge their password to anyone else.
- **Device Sharing/Staff Sickness/Re-assigning a laptop** – A laptop can be re-assigned to another user or more than one user can be assigned to it. This is covered in chapter 9.
- **Supply Teachers** – We recommend that the school uses curriculum laptops with no sensitive data for supply teacher use. If you have a regular supply teacher or one on a longer term they should be set up with their own Encryption service username following the steps in chapter 9.
- **Laptop replacement** – if a laptop is replaced in school the encryption software will need to be removed before it can be put onto the replacement to avoid duplicate charges - see Appendix A for guidance.
- **Laptop Repair** – If a laptop is repaired under warranty, depending on the part replaced you may not need to do anything in regards to encryption. See Appendix A guidance.
- **Backup** – it is vitally important that data on an encrypted laptop is backed up regularly. This becomes even more important than before because data recovery is not possible on an encrypted hard disk

If you find areas we have missed please send us an email (mailto:systems@devon.gov.uk) so we can improve our documentation.

Chapter 3 – Billing and charging

Please note that this information is based on the initial offer pricing which is correct and valid until the 31st of March 2010. For current prices visit http://www.scomis.org/go/encryption.

Each mobile/laptop device on the service is subject to a one off charge and an annual charge:

- The one-off initial cost per device will be charged as and when devices are added to the service throughout the year
- The annual cost per device will be charged at the beginning of the school's financial year for existing devices.
  - For devices added throughout the year they will be charged on a pro-rata basis as and when they are added

Additional Devices

Throughout the year you may need to add additional devices onto the service. To do this simply visit http://www.scomis.org/go/encryption and submit an additional order for the extra devices you need.

Check the current pricing as it may well have increased following the initial offer.

After submitting your order you can proceed to install onto your new devices.

Important Note

- The installation routine allows you the flexibility to add additional devices as needed so will **not** stop you from installing onto more devices than you originally ordered.
- Each month we will compare the number of devices on the service against the number ordered by your school.
  - Where there are more devices than we have received orders for we will give you the option of submitting an order for the additional devices or having them decrypted and therefore unprotected.

Chapter 4 – Preparing to implement encryption

Once you have received your email with your school's unique installation key the software will have been released to you for download from the ScoMIS upgrades website

1. **Downloading the ScoMIS Encryption Service Setup package – follow the notes below or watch this screen cast video http://faq.scomis.org/kb541/**
   a. Visit http://www.scomis.org/go/scomis and navigate to "Download Upgrades" using the link on the left hand side
   b. Log in with your full school cost code
   c. Click "download and store" on the "ScoMIS Encryption Service Installer Download"
   d. Choose Yes, Install, Proceed or Run to any security warnings or questions you are asked
   e. There maybe a delay from when you click on the link to the wizard starting up because the setup package is 15mb and has to be downloaded onto you computer
   f. Choose "Next, Next, Next and Install" to the choices in the installation wizard and click "Finish" once the option appears

      Note: If you have problems with the setup wizard never starting after you click on the link you could have a popup blocker or problems with your temporary internet files. First try holding down **Ctrl** when clicking the link and keeping it held down until the Setup wizard asks if you want to install the package. If it still fails you can try emptying your temporary internet files (http://support.microsoft.com/kb/260897). If you still have problems you will need to log a call with the service desk

2. **Putting the ScoMIS Encryption Service Setup Package on the network – follow the notes below or watch this screen cast video http://faq.scomis.org/kb545/**
   a. The first step downloads the package your C:\ drive, next you need to put it onto the network so that your users can access it.
   b. Open up "My Computer" and double click into your C:\ drive

c. Select the “ScoMISEncryptionService” folder, click “Edit” and choose “Move to Folder…”

d. Browse to a suitable network location, this should be a network drive or folder that your teachers and staff have access to but **the pupils do not**.

e. As an alternative or in addition to putting the setup package on your network it could also be copied onto a USB Drive; in this case follow the same steps but insert the USB Drive and browse to it during step d.

f. Note down the location for later use, e.g. “*R:\Resources\Software Packages\ScoMISEncryptionService\ScoMISEncryptionServiceSetup.exe”* as you will need to communicate this to your users

Chapter 5 – Implementing the encryption software

We recommend you carry out an initial pilot installation onto your own laptop, if you do not have your own laptop watch this screen cast video of the process http://faq.scomis.org/kb550/. Having done this you should be able to choose which of the following options will be best for you based on your user's confidence and experience with ICT.

1. **End user installation (recommended for most Primary Schools)** – This involves each user completing the installation themselves as per the installation guide. It maybe that you want to edit the guide so that it is more specific to your school for example adding specific instructions to replace the chapter on backup
2. **Assisted Installation** – This involves you or a confident person in ICT who has carried out the installation on their device sitting with each user as they complete the installation. It maybe that you could do this for final installation stage leaving the user to carry out their own backup and CHKDSK depending on your users confidence and ability with ICT
3. **Technician Installation (recommended for Secondary and Primary Schools with full time ICT Technician)** – This involves the user leaving the laptop with the technician for them to carry out the installation. Once this is complete the user need only spend 20 minutes with the technician to be enrolled onto the service. For further guidance following this route download the Secondary School documentation from http://www.scomis.org/go/encryptiondocs.
4. **ScoMIS Installation** – We do hot have a dedicated resource available for encryption installation however; schools who purchase regular tech time may wish to use some of this time to have the work completed and we may be able to book installations for other schools but this will have to be worked around our existing commitments.
    a. To make the most out of this you should ensure if at all possible that the users themselves carry out the backup and CHKDSK stages of the installation
    b. They will also need to bring their laptop into school for the visit and be available for 20 minutes at some point in the day so they can be enrolled onto the service

Chapter 6 – Implementation Checklist

Mark off the tasks are they are completed to make sure you keep on track and have a successful and smooth rollout of encryption in your school

Who	Task	Done?
School	Decide how many devices/laptops you need to have encrypted. We recommend that initially all teacher and administration laptops are encrypted. An online calculator is available at http://www.scomis.org/go/encryption which shows you the initial and ongoing annual cost for your school	
School	Submit your order to ScoMIS through the online order form at http://www.scomis.org/go/encryption for the amount of devices you want to protect	
ScoMIS	Send documentation to school & release software	
School	Read the Deployment Guide	
School	Familiarise yourself with the installation guide and process	
ScoMIS	Send unique installation key to school. **Remember** we will be carrying out a phased rollout during the initial launch to maintain high levels of service. This may mean there is a delay between the time between you receive the documentation and installation key	
School	Download setup package to school network	
School	Carry out pilot installation	
School	Make any customisations to the Installation guide specific to your school e.g. you may want to alter the guide to advise users to backup their files to a specific location on the network	
ScoMIS	If you have queries that aren't answered in the documentation or come across issues which may affect your users during installation please log a call with the ScoMIS Service Desk before moving onto the next stage	
School	Send the Installation Guide, Installation Key, Setup location to your users.	
Installations can now begin in school		

Chapter 7 – Getting help and support

If a user is having problems logging onto their laptop; for example if they have forgotten their password:

1. First attempt local recovery following the onscreen instructions in the pre-boot login screen
2. If successful this will let them choose a new password and enable them to log back onto their laptop

If they have problems with local recovery they should **telephone the ScoMIS Service Desk on 01392 385300.** We will go through a short recovery process and reset your password after completing an identity check based on the questions set during your account creation. If you forget your security questions we will still be able to reset your password but only by us calling the main school number to confirm your identity.

The ScoMIS Service Desk is open from 8am until 6pm during school term (8am to 5pm on Fridays) and 9am until 5pm during school holidays.

For non urgent issues or queries please:

1. Check the next chapter which covers common questions and answers
2. Check the ScoMIS website which will be kept up to date with FAQ's and the latest versions of the documentation

If your query is not answered in our user guide or website please log a call us. You can either telephone on 01392 385300 or send us an email to scomis@devon.gov.uk to log a call.

We also welcome feedback on the documentation provided for encryption service. If you have any suggestions for improvements please send us an email to systems@devon.gov.uk – please note this is a feedback address and should not be used to log issues or calls for assistance

Chapter 8 – Answers to common questions / FAQ's

- How do I know that a device is encrypted?
    - If the encryption software is installed you will see the McAfee login screen before Windows loads
- How do I remove or reinstall the encryption software?
    - See **Appendix A** in this guide
- What happens if device hardware is upgraded?
    - Added RAM will not affect encryption however upgrading the hard disk will mean that you need to contact ScoMIS for advice
- My users will want an easier to remember password?
    - All devices and users on the ScoMIS Encryption Service must adhere to the DCC Password policy.
    - A strong and hard to guess password does not necessarily need to be hard to remember for example you could use a line from a favourite song: **Never4getWhereYou'veComeHereFrom**
    - Alternatively try generating one with the memorable password generator > http://www.safepasswd.com/
- What happens if a laptop needs to be re-assigned to a different member of staff due to long term sickness for example
    - Use the maintenance utility as explained in Chapter 9 to add a new or existing user and reassign the device.
    - If you are unable to log onto the device because the only user normally able to is out of school log a call with the ScoMIS Service Desk
- What happens if Windows needs to be re-installed due a corruption or virus attack?
    - See **Appendix A** in this guide
- Does encryption protect against viruses?
    - No you still need up to date antivirus software installed because the encryption software is totally transparent to windows
- Where can I find out more information?
    - Check http://faq.scomis.org/categories/services/encryption
    - Log a call with the ScoMIS Service Desk for any other queries

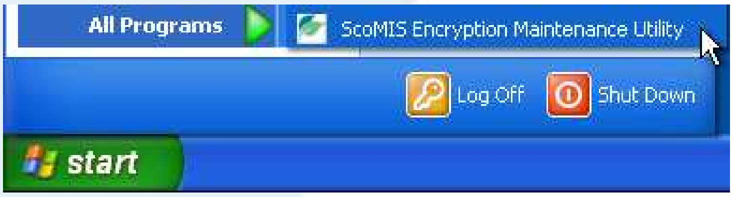
Chapter 9 – The ScoMIS Encryption Maintenance Utility

ScoMIS have included a maintenance utility to allow you to carry out the following tasks:

- **User Maintenance**
  - **New user** - create a new user and assign to the machine
  - **Existing user** – assign an existing user to the machine
  - **Group** – assign multiple existing users to the machine, you may choose to add all users to all devices if they are regularly shared for example
- **Reassign device**
  - Allows you to update the device description in our database
- **View DCC Password Rules**
  - Used when creating a new user so that you can explain the password policy before they attempt log on for the first time
- **Force Synchronisation**
  - Should be run after making any changes using the functions above, this pulls down the settings to the device from the central database

To launch the utility go to:

Start > All Programs > "**ScoMIS Encryption Maintenance Utility**"



Notes:

- A "new user" means one that doesn't already have a login for the encryption service, if they use another encrypted device use the "existing user" option to allow them access to the device in question
- The user maintenance functions are protected and require you to enter the schools unique installation key, if this has been lost or forgotten please log a call with the ScoMIS Service Desk
- Depending on your windows security settings you may need administrator rights to run this application
- If you have any problems or see any errors using this application please note them down or take a screen shot and log a call with the ScoMIS Service Desk

Appendix A – Removing or re-installing the encryption software

Once installed the encryption software cannot be removed by the end user or school. To remove the software you will need to log a call with the ScoMIS Service Desk.

If the encryption software needs to be re-installed for example following a repair after hardware failure please log a call with the ScoMIS Service Desk. We will need to manually delete the old device from our database to avoid the school being charged for a duplicate device.

Common reasons for removing the software may include

- A laptop is due to be replaced – the encryption software should be removed so it can be installed onto the replacement device without the school incurring a duplicate charge
- The security profile of the laptop has changed – Our advice is to encrypt all teacher and administration laptops. If a laptop changes role to be used in the curriculum, by pupils or supply teachers for example the encryption software should be removed

Common reasons for re-installing the software may include

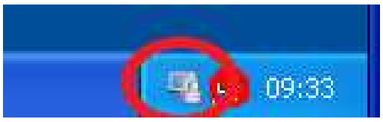
- Windows has become corrupted – you will need to re-install the encryption software after re-installing the Windows operating system
- Hardware Failure – if the laptop hard drive fails you will need to re-install the encryption software after the fault has been rectified

Please Note: It is possible to reinstall the Windows operating system by using the installation CD or running a recovery mechanism such as a ghost reload. This will mean there is no encryption on the hard drive however the original data will remain encrypted and still be secure.

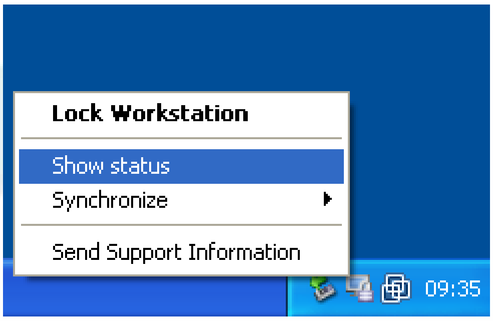
Appendix B – Installation in an RM CC3/CC4 network

The encryption software has been tested and is known to work on RM CC3/CC4 network laptops. Once installed it will not affect Windows or the RM network as encryption is totally transparent.

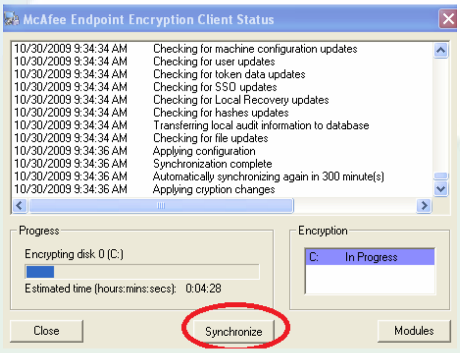
- The installation has to be carried out manually because it cannot be packaged
- You will need to log on with a System Admin user account to do the installation, after installation the user will log on as normal
- During the 1st restart of installation the forced synchronise stage may not work as described in the notes. In this case you need to manually force a synchronisation then restart the computer, to do this:
    - Once the Desktop has loaded right click on the Encryption Padlock icon the system tray

      then left click on “Show Status”

      finally click synchronise then once the progress bar has appeared to indicate the encryption process has begun restart the computer to continue with the installation

      McAfee Endpoint Encryption Client Status

      ```
      10/30/2009 9:34:34 AM     Checking for machine configuration updates
      10/30/2009 9:34:34 AM     Checking for user updates
      10/30/2009 9:34:34 AM     Checking for token data updates
      10/30/2009 9:34:34 AM     Checking for SSO updates
      10/30/2009 9:34:34 AM     Checking for Local Recovery updates
      10/30/2009 9:34:34 AM     Checking for hashes updates
      10/30/2009 9:34:34 AM     Transferring local audit information to database
      10/30/2009 9:34:34 AM     Checking for file updates
      10/30/2009 9:34:36 AM     Applying configuration
      10/30/2009 9:34:36 AM     Synchronization complete
      10/30/2009 9:34:36 AM     Automatically synchronizing again in 300 minute(s)
      10/30/2009 9:34:36 AM     Applying cryption changes
      ```

      Progress: Encrypting disk 0 (C:)

      Estimated time (hours:mins:secs):   0:04:28

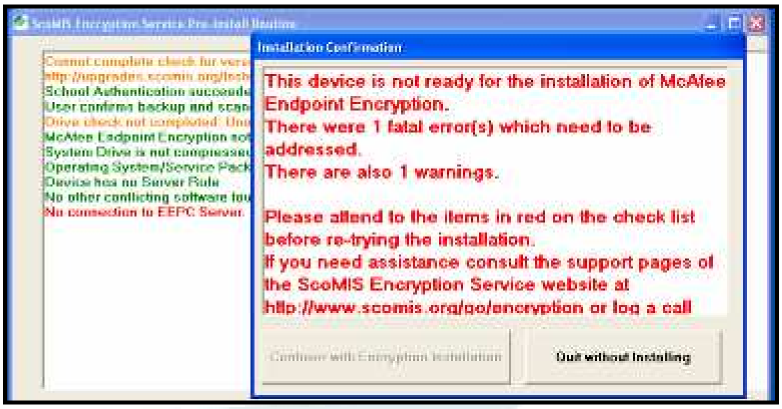
      Encryption: C: In Progress

- If a machine is rebuilt then log a call with the ScoMIS Service Desk before reinstallation to avoid being charged for a duplicate device

Appendix C – Installation in a Viglen Classlink network

There are no known issues with the default Viglen Classlink Network configuration and the ScoMIS Encryption Service.

It is possible that customer ISA Firewall rules in place which are outside of the default network install could effect the installation. In this situation the installation routine will notify you that it can't communicate with the ScoMIS Encryption Server.


ScoMIS Encryption Service Pre-Install Routine
Installation Confirmation
Continue with Encryption Installation
Quit without Installing

```
Cannot complete check for vers
http://upgrades.scomis.org/tech
School Authentication succeede
User confirms backup and scan
Drive check not completed: Una
McAfee Endpoint Encryption not
System Drive is not compressed
Operating System/Service Pack
Device has no Server Role
No other conflicting software fou
No connection to EEPC Server.
```

This device is not ready for the installation of McAfee Endpoint Encryption.
There were 1 fatal error(s) which need to be addressed.
There are also 1 warnings.

Please attend to the items in red on the check list before re-trying the installation.
If you need assistance consult the support pages of the ScoMIS Encryption Service website at http://www.scomis.org/go/encryption or log a call

If you carry out our recommended rollout plan you should find this issue on the first device you attempt installation on. In this case please log a call with the ScoMIS Service Desk so that it can be resolved before attempting installation on any other devices.

Appendix D – How the encryption software works

On protected devices for example Laptops or PCs, the client side of Endpoint Encryption, in simple terms, takes control of the user's hard disk away from the operating system. Endpoint Encryption's driver encrypts every piece of data written to the disk, and decrypts every piece of information read off the disk. If any application managed to break through the Endpoint Encryption barrier and read the disk directly, it would find only encrypted data, even in the Windows swap file and temporary file areas.

Even if a Data Recovery agency tries to retrieve information from a Endpoint Encryption-protected hard drive, without access to the Endpoint Encryption System via the passwords or recovery information there is no way of accessing this data – total security.

Endpoint Encryption installs a mini-operating system on the user's hard drive, this is what the user sees when they turn on the PC. Endpoint Encryption looks and feels like Microsoft Windows, with mouse and keyboard support, moveable windows etc. This Endpoint Encryption OS is completely contained and does not need to access any other files or programs on the hard disk, and is responsible for allowing the user to authenticate with their password.

Once the user has entered the correct authentication information, the Endpoint Encryption operating system starts the crypt driver in memory, and boots the protected machine's original operating system. From this point on, the machine will look and behave as if Endpoint Encryption was not installed. The security is invisible to the user, and because the only readable data on the hard disk is the Endpoint Encryption operating system, and the encryption key for the hard drive is itself protected with the user's authentication key, the only possible way to defeat Endpoint Encryption is to either guess the hard disk encryption key (a one in 2256 chance with the AES256 algorithm), or to guess the user's password.

Every time an Endpoint Encryption protected device boots, and after a set period of time, Endpoint Encryption tries to contact its "Object Directory". This is a central store of configuration information for both machines and users, and is managed by Endpoint Encryption Administrators. The Object Directory could be on the user's local hard disk (if the user is working completely stand-alone), or could be in some remote location and accessed over TCP/IP via a secure Endpoint Encryption Server (in the case of a centrally managed enterprise).

The Endpoint Encryption protected machine queries the directory for any updates to its configuration, and if needed downloads and applies them. Typical updates could be a new user assigned to the machine by an administrator, a change in password policy, or an upgrade to the Endpoint Encryption operating system or a new file specified by the administrator. At the same time Endpoint Encryption uploads details like the latest audit information, any user password changes, and security breaches to the Object Directory. In this way, transparent synchronization of the enterprise becomes possible.