

SecureClient Central – Installation Guide

September 2014

Table of contents

1. About this guide	5
2. System requirements	6
3. Installation	7
4. Software upgrades	12
Appendix 1 - Notes for the IT Department	13
1. Having multiple instances of SecureClient installed	13
2. Network deployment	13
3. Proxy and firewall settings	13

1. About this guide

This guide describes the process to download and install the SecureClient application for SecureAssess Central.

SecureClient must be installed in every machine that will be used by learners to sit exams.

Important note: Please ensure that your IT department is aware before installing this software manually.

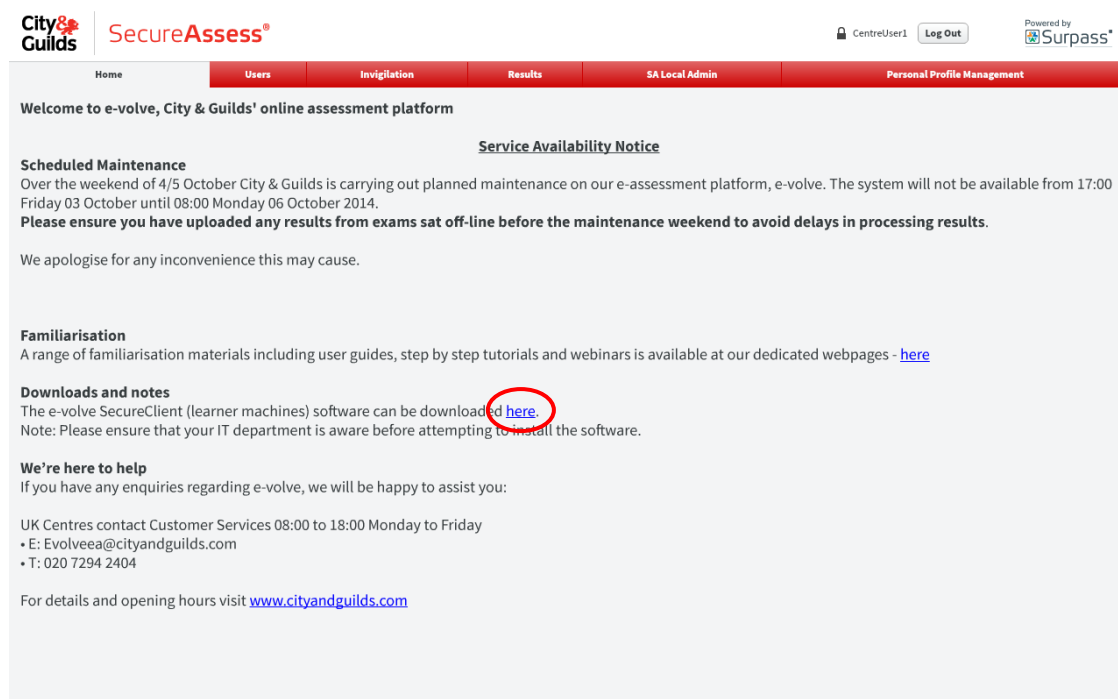
2. System requirements

These are the **minimum technical requirements** and **supported platforms** for installing and running SecureClient Central.

Hardware	
Processor	2.33GHz or faster x86-compatible processor For exams containing Advanced Question Types (includes Functional Skills and Principles of English and Maths assessments), we recommend that Celeron processors are avoided.
Hard Drive Space	1GB
Memory (RAM)	1GB For exams containing Advanced Question Types (includes Functional Skills and Principles of English and Maths assessments), this should be increased to 2GB.
Video	Single display Screen resolution of 1024x768 Graphics card with at least 128MB of memory
Peripherals	Two button mouse Keyboard Audio capability and headphones may also be required for some assessment types
Software	
Operating System	Windows XP (Service Pack 3) – Comes to end of supported life April 2014 Windows 7 (32-bit or 64-bit) Windows 8 (32-bit or 64-bit)
.NET	Microsoft .NET Framework 2.0 (Service Pack 2) to Microsoft .NET Framework 4.0
Internet browser	Internet Explorer 7 to 10 <i>Adobe Reader must be installed and enabled for the browser</i>
Adobe Flash Player	Adobe Flash Player 10.3 to 11.7.700.224 <i>This needs to be the ActiveX version of flash i.e. it needs to have been installed from Internet Explorer.</i>
Bandwidth	
Minimum Requirements	An internet connection of 2Mbps or greater for every 30 candidate tests being sat at the same time is recommended to ensure candidates are not affected by connection issues during exam delivery. You are advised to use the Advance Download functionality if you do not want candidates to have to wait for the exam to download at the start of the session. Advance Downloaded exams must be sat without an internet connection. The use of 3G cards may not guarantee a constant bandwidth and could therefore not meet the minimum requirements. The use of these cards is not supported.

3. Installation

Step 1
Go to
SecureAssess
Central
Homepage
and follow the
link to
download
SecureClient.



City & Guilds SecureAssess®

CentreUser1 Log Out

Powered by Surpass®

Home Users Invigilation Results SA Local Admin Personal Profile Management

Welcome to e-volve, City & Guilds' online assessment platform

Service Availability Notice

Scheduled Maintenance
Over the weekend of 4/5 October City & Guilds is carrying out planned maintenance on our e-assessment platform, e-volve. The system will not be available from 17:00 Friday 03 October until 08:00 Monday 06 October 2014.
Please ensure you have uploaded any results from exams sat off-line before the maintenance weekend to avoid delays in processing results.

We apologise for any inconvenience this may cause.

Familiarisation
A range of familiarisation materials including user guides, step by step tutorials and webinars is available at our dedicated webpages - [here](#)

Downloads and notes
The e-volve SecureClient (learner machines) software can be downloaded [here](#).
Note: Please ensure that your IT department is aware before attempting to install the software.

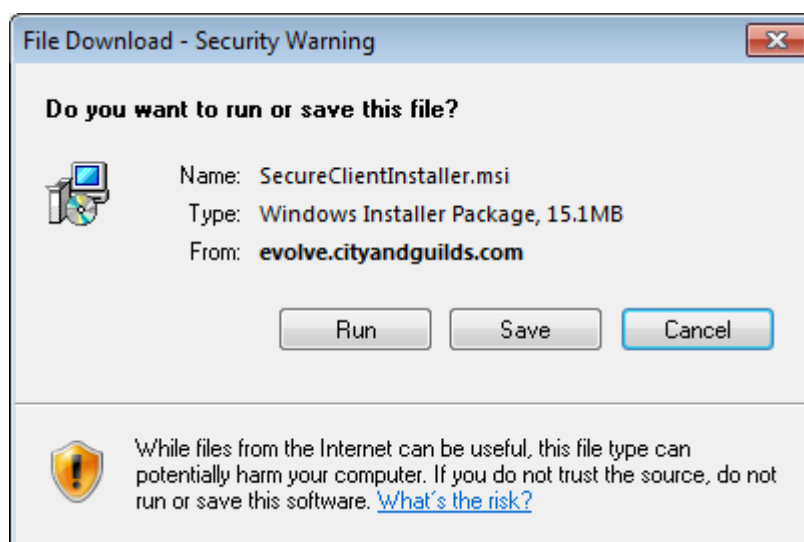
We're here to help
If you have any enquiries regarding e-volve, we will be happy to assist you:

UK Centres contact Customer Services 08:00 to 18:00 Monday to Friday
• E: Evolveea@cityandguilds.com
• T: 020 7294 2404

For details and opening hours visit www.cityandguilds.com

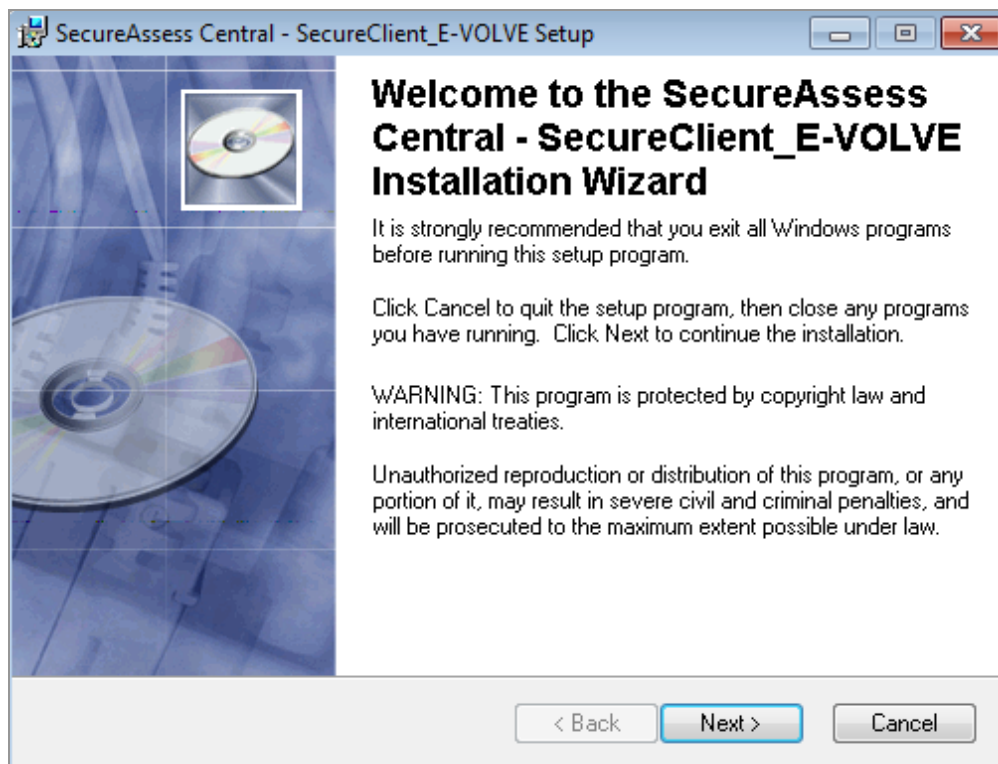
Step 2

Once the file has downloaded double click it. A security warning will then pop up. It will say that the publisher could not be verified. This is a routine security step to prevent unwanted software installing itself, by requiring confirmation from the computer's owner. Click **Run**.



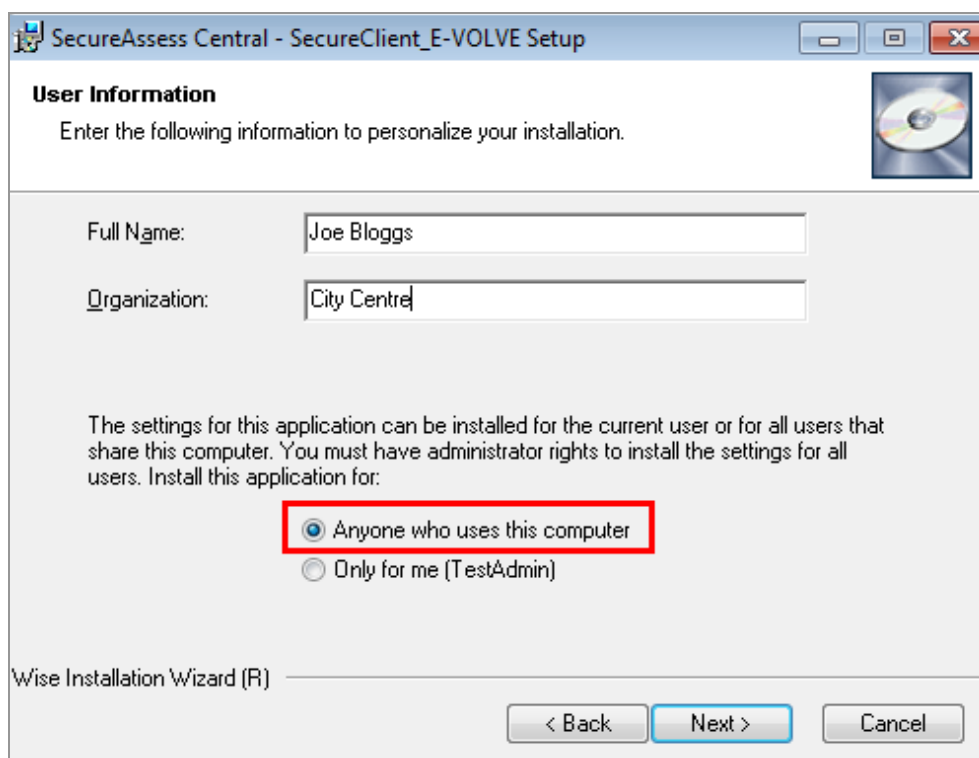
Step 3

When the SecureClient Installation Wizard opens, click **Next**.



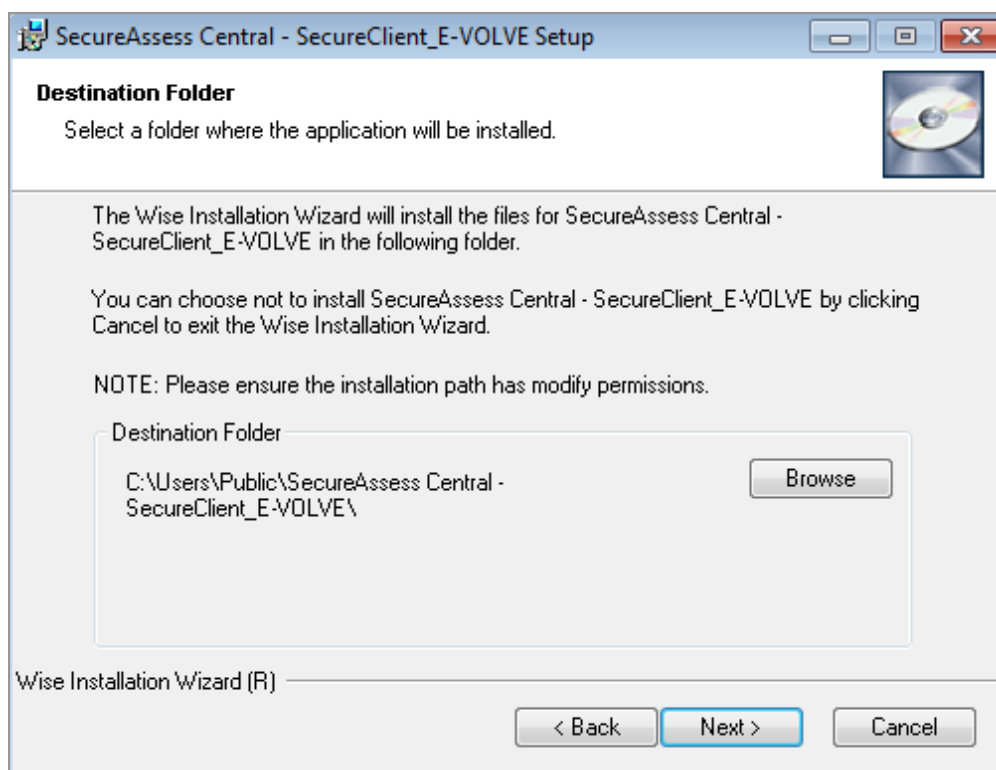
Step 4

You will be asked for your name and Organisation information – this is optional. Make sure you **always** select '**Anyone who uses this computer**'. Click **Next** to proceed.



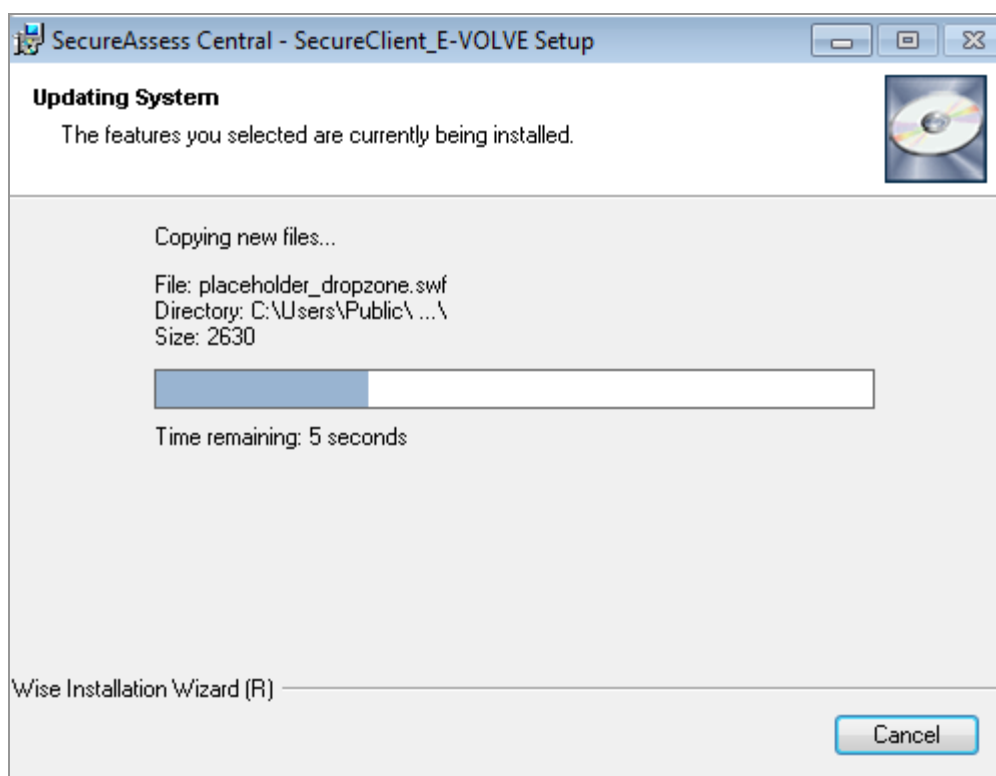
Step 5

You will be shown the folder where the SecureClient application will be installed. Unless specified to do otherwise please leave this as it is. Click **Next** to proceed.



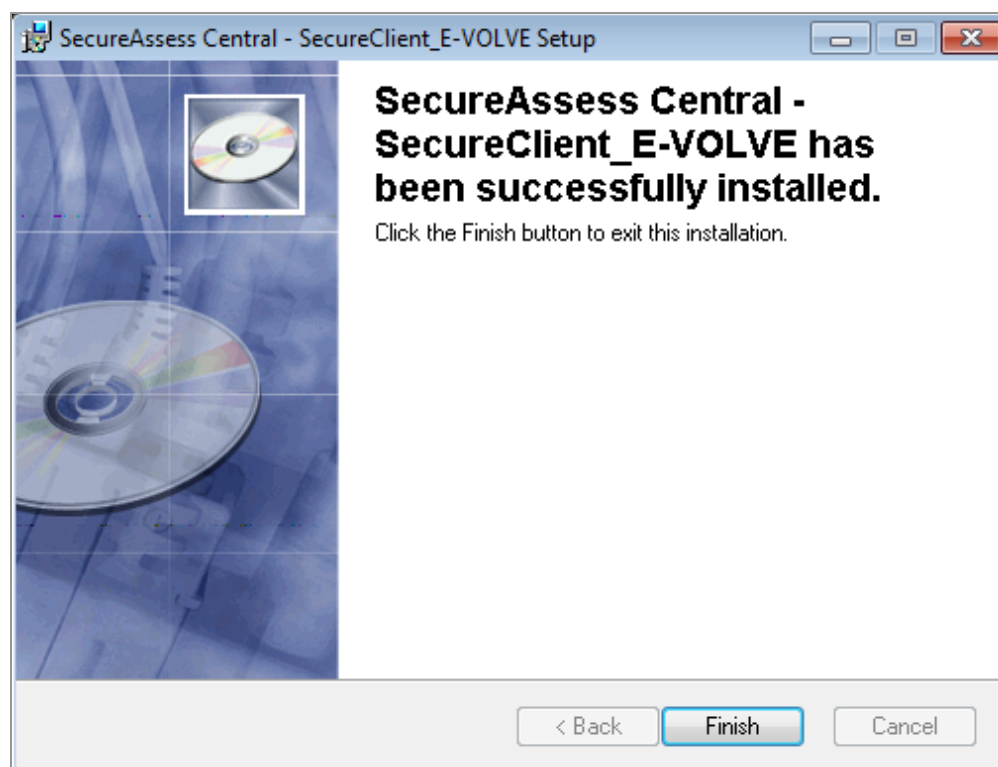
Step 6

The installation will start and a progress bar will be displayed throughout. You do not need to take any action. If you click 'Cancel', the installation will stop.



Step 7

A final screen confirms that the installation is complete. Click **Finish** to exit.



The installation is now complete. An icon to launch SecureClient will have been created on your desktop. The icon looks like this:



Step 8

Run a navigation test to check that the installation was successful.

4. Software upgrades

Once the software is installed any further upgrades happen automatically and they will not require administrative rights. This is done via a simple check when the software starts. When this occurs, you may notice the software taking slightly longer to open.

Appendix 1 - Notes for the IT Department

This section is only relevant for staff at the IT Department. It deals with specific technical aspects of the installation which may be applicable in some cases.

1. Having multiple instances of SecureClient installed

SecureClient has to be installed in every testing station, even if you already use BTL Surpass software with another awarding body. It will not interfere with any other pre-existing e-assessment solutions you use, even if you already have installed another instance of SecureClient.

2. Network deployment

SecureClient installer is a single MSI, so you can distribute and install it over your network using normal MSI deployment methods (i.e. quiet mode).

3. Proxy and firewall settings

Your Proxy Server

Proxies and/or firewalls may need to be configured to allow access to the SecureAssess Central server. Configure the proxy to not require authentication for communications to:

<https://evolve.cityandguilds.com> (Port 443 and 80)

<http://evolve.cityandguilds.com> (Port 443 and 80)

These URLs should also be added to the safe list of any firewalls.

Proxies should also be configured to allow ASMX, ASPX and ZIP file types.

Your testing stations (SecureClient)

SecureClient will automatically mirror the proxy settings you have made in Internet Explorer. However, if Internet Explorer is configured automatically via a script, SecureClient will not mirror it and you will need to enter the details manually. You will be prompted to do so when you launch it for the first time.

If you are prompted **every time** you launch SecureClient, or you see the message "*The current Secure Client has updates that are invalid. Please contact your local administrator*" when you attempt to launch it, you will need to manually configure SecureClient with your Proxy settings (see below).

Manually configure SecureClient with your Proxy settings

The following process will configure a single SecureClient application to your proxy settings.

1. Go to the the **configfiles** folder in the SecureClient install directory and open the **Proxy.xml** file using Notepad. The default install directory is as follows, unless you have chosen a different one:
 - **Windows XP** – C:\Documents and Settings\All Users\Application Data\securssess\SecureAssess Central - SecureClient_E-VOLVE\configfiles
 - **Windows Vista & 7** – C:\Users\Public\SecureAssess Central - SecureClient_E-VOLVE\
2. Enter the **proxy server address and port number** in proxy.xml. For example if your proxy server address is '172.1.1.1 on port 8080', the text in proxy.xml should look like this:

```
<proxy><useProxy>true</useProxy><server>172.1.1.1</server><port>8080</port><validationRequired>false</validationRequired><user></user><password></password></proxy>
```

3. If your proxy server requires **user validation** you should also enter the **user information**. Using the same example, if your proxy server requires you to login with the username 'name' and the password 'pass', the text in proxy.xml should look like this:

```
<proxy><useProxy>true</useProxy><server>172.1.1.1</server><port>8080</port><validationRequired>true</validationRequired><user>name</user><password>pass</password></proxy>
```

If you have a large network of computers running SecureClient, you could **roll out these settings across your network**. If you have a network which is capable of executing a script to 'copy and paste (overwrite)' onto each computer in the network you can simply paste the edited proxy.xml file into the configfiles folder within the SecureClient install directory on every learner machine.