

SecureClient Central: Installation Guide

September 2011

Table of contents

1. About this guide	3
2. System requirements	4
3. Installation	5
4. Software upgrades	9

Appendix 1 – Notes for the IT Department	10
1. Having multiple instances of SecureClient installed.....	10
2. Network deployment.....	10
3. Proxy and firewall settings.....	10

Require further assistance?

Contact the City & Guilds dedicated e-volve migration team on:

Tel: **020 7294 2898**

Email: e-volve.migration@cityandguilds.com

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 candidates 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 speed	2.33GHz Single core CPU, or 1.2GHz Dual core CPU
Memory (RAM)	1GB
Hard Drive	1GB of free space
Display	1024 x 768 screen resolution
Software	
Operating system	Windows XP (SP3 or later), or Windows Vista (32-bit or 64-bit), or Windows 7 (32-bit or 64-bit)
.NET	Microsoft .NET Framework 2.0 (Service Pack 2 or later), or Microsoft .NET Framework 3.0 (Service Pack 2 or later), or Microsoft .NET Framework 3.5 (Service Pack 1 or later)
Internet browser	Internet Explorer 7 or 8
Adobe Flash Player	Adobe Flash Player 10* *This needs to be the ActiveX version of Flash i.e. it needs to have been installed from Internet Explorer.
SQL Server Compact	SQL Server Compact 3.5 (Service Pack 1 or later)* *SQL Server Compact 3.5 Service Pack 2 can be downloaded from: http://www.microsoft.com/download/en/confirmation.aspx?id=5783

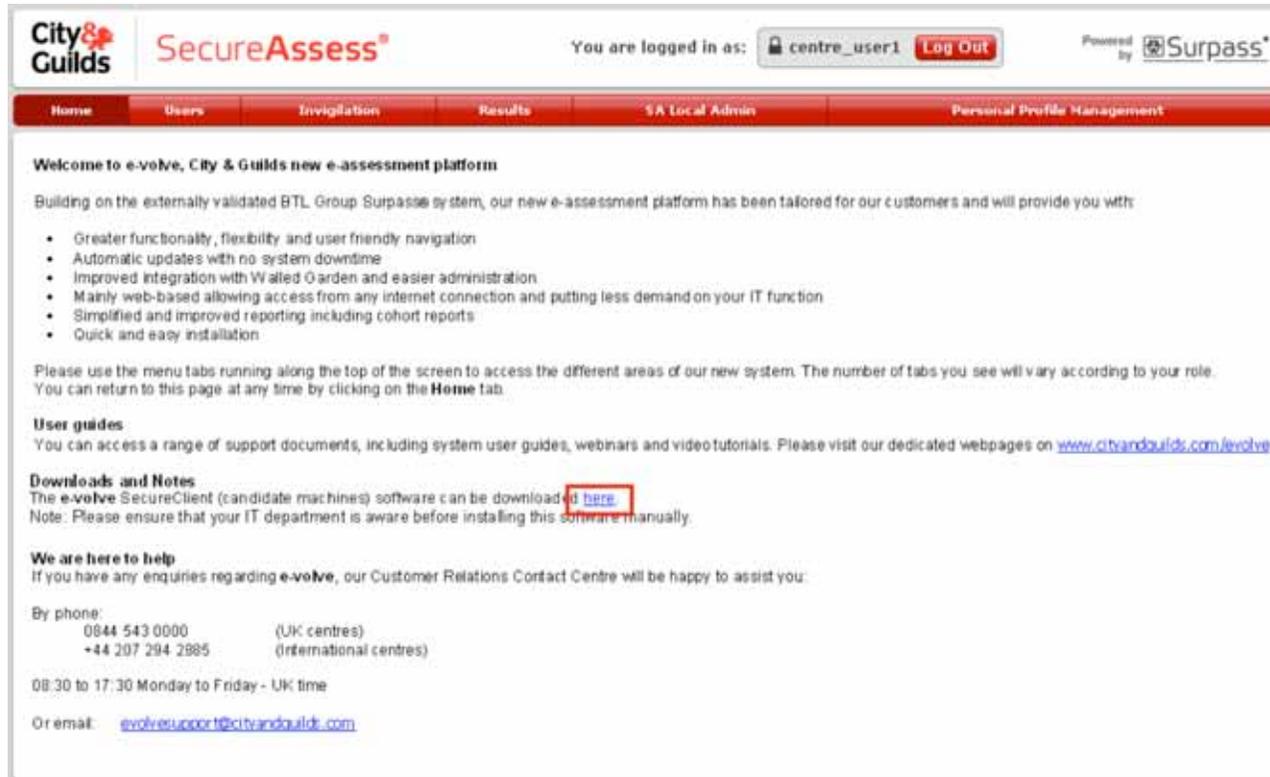
Internet connection and bandwidth

Permanent internet connection with 512 Kbps per 10 concurrent exams being taken. Please note that the use of 3G cards may not guarantee a constant bandwidth and could therefore not meet the minimum requirements.

3. Installation

Step 1

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



The screenshot shows the SecureAssess Central Homepage. At the top left is the City & Guilds logo. Next to it is the 'SecureAssess' logo. On the right, it says 'You are logged in as: centre_user1' with a 'Log Out' button. Further right, it says 'Powered by Surpass'. Below the header is a navigation menu with tabs: Home, Users, Invigilation, Results, SA Local Admin, and Personal Profile Management. The main content area starts with a welcome message: 'Welcome to e-volve, City & Guilds new e-assessment platform'. It then lists several bullet points: Greater functionality, flexibility and user friendly navigation; Automatic updates with no system downtime; Improved integration with Walled Garden and easier administration; Mainly web-based allowing access from any internet connection and putting less demand on your IT function; Simplified and improved reporting including cohort reports; Quick and easy installation. Below this, it says 'Please use the menu tabs running along the top of the screen to access the different areas of our new system. The number of tabs you see will vary according to your role. You can return to this page at any time by clicking on the Home tab.' There are sections for 'User guides' (with a link to www.cityandguilds.com/evolve) and 'Downloads and Notes' (with a link to download SecureClient software). The 'Downloads and Notes' section includes a note about manual installation and contact information for support, including phone numbers for UK and international centres, and an email address: evolvesupport@cityandguilds.com.

Step 2

When the page loads, click on: 'Click here to download SecureClient Installer' and save the installer to your computer.

Step 3

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**.



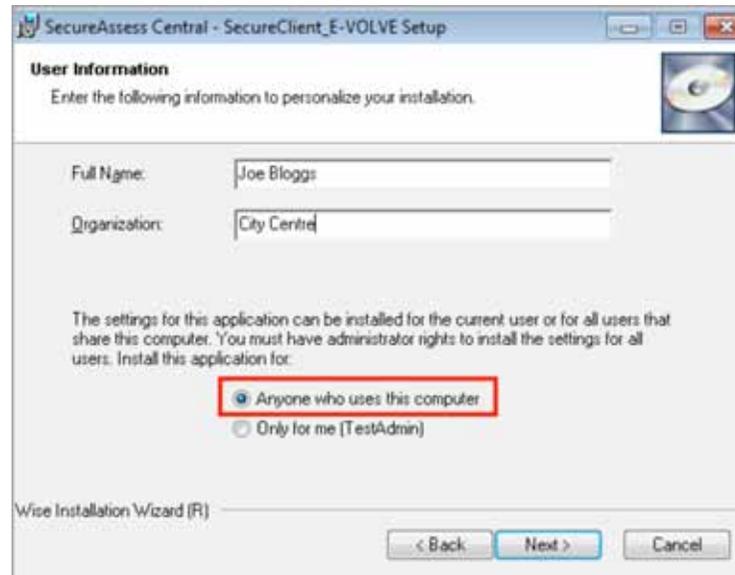
Step 4

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



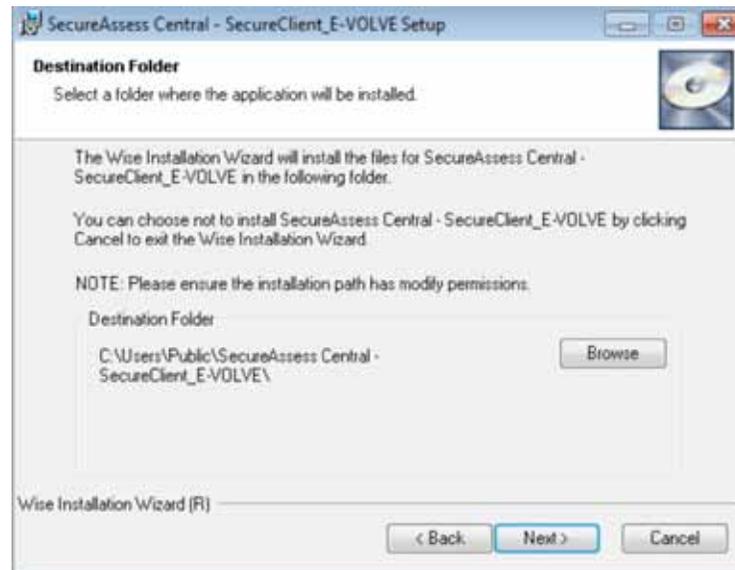
Step 5

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.



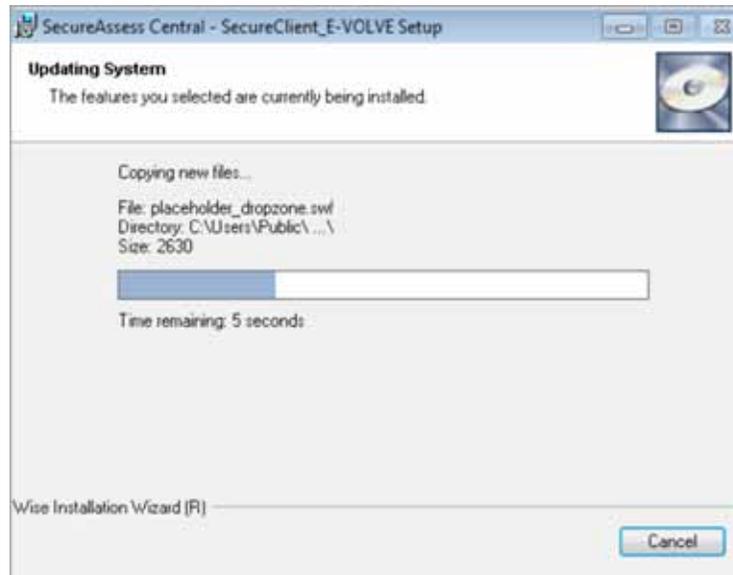
Step 6

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 7

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 8

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 9

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. City and Guilds will still communicate all upgrades to you well in advance of them happening so you have time to co-ordinate.

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 examining 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 examining 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 candidate machine.