Surpass®

SecureAssess Local

Install Guide

Release 9.0

Document 1.0 15.11.10

btl learning & assessment

www.btl.com

Disclaimer

Whilst every effort has been made to ensure that the information and content within this user manual is accurate, up-to-date and reliable, the information provided is on an “as is” basis. BTL shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this manual or from the use of the software accompanying it.

Please note that screenshots may differ slightly in graphical style from those in your system. This is because graphics have been customised for the client by BTL. The layout and functionality of the screens in this manual will be consistent with your system.

Contents

Contents 3
About this Guide 5
BTL Service Desk Contact Information 5
Before you begin the installation 6
Notes on the installation 6
Notes on the System Requirements 7
Installation 7
Step by Step Guide to Installing SecureAssess Local 9
The Configuration Wizard/Error 997 16
Configuration Wizard 17
Using SecureAssess Local 21
Offline Administrator 21
Proxy Details 21
Installation Log 22
Configuration 23
Synchronise Centre 24
System Information, Data Report and Error Log tabs 25
System Information 25
Data Report 26
Error Log 27
Appendix 1: Diagnostics Page 28
Appendix 2: Installing Microsoft Internet Information Services (IIS) 6.0 29
Installing IIS 29
Appendix 3: Installing .NET Framework 30
A note on IIS and .NET 30
The install procedure for the .NET framework 30
Appendix 4: Installing SQL Server 2005 Express Edition 31
Mixed Mode Authentication 31
Enabling Mixed Mode Authentication on an existing installation of SQL Server 2005 Express Edition 32
Appendix 5: Enabling ASP.NET & Active Server Pages 35
Appendix 6: Configuring SecureAssess Local to operate on a new website 36
Create New Website/Virtual Directory 36
The Web Site Creation Wizard 37
Create a New Application Pool 40
Set the Properties of the Website to use the new Application Pool 41
Appendix 7: Configuring SecureAssess Local to operate on a custom port 43
Manual Changes to Configuration files for a Custom Port Number 43
Windows Service 44
Web Directory 45

Appendix 8: Changing the IUSR Account in IIS 47
Document Change Record 52

About this Guide

This guide will give you the information you need to install SecureAssess Local at your centre. This guide contains all the core information about installing, configuring and testing the SecureAssess Local system.

You should familiarise yourself with the information in this guide before installing SecureAssess Local.

BTL Service Desk Contact Information

If there is anything that you need to know that isn't covered here, or you require any extra support, you should contact BTL's Service Desk.

Email: support@btl.com

Telephone: 01274 203 270

Before you begin the installation

Make sure that you have installed and configured the following before beginning the SecureAssess Local Installation.

1. Install Microsoft Internet Information Services (IIS) 6.0.
   You will also have to configure Active Server Pages and ASP.NET as 'Allowed'.

   Information on these procedures can be found in Appendix 2 and Appendix 5 respectively.

2. Install Microsoft .NET Framework.
   Information on this procedure is located in Appendix 3.

3. If you don't have an existing SQL database, install Microsoft SQL Server 2005 Express.
   If you are using an existing SQL server, ensure that mixed mode authentication is switched on.

   Information on this is located in Appendix 4.

4. 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://[organisation].secureassess.co.uk. This URL should also be added to the safe list of any firewalls.

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

   Firewalls should allow access to the SecureAssess central server on port 443

   You may have to contact your managed service provider to do this

5. Check that the Default Web Site is operational
   If the default Web Site is disabled or not available you should create a new Web Site in IIS.

   Information on this is located in Appendix 6.

6. Check that port 80 is available
   If port 80 is in use by another website then you should configure SecureAssess Local to use a custom port number.

   Information on this is located in Appendix 7.

Notes on the installation

This installation will create a virtual directory named 'secureassesslocal' within the Default Web Site of the server. The base URL for the site will be: http://[servername]/secureassesslocal/

Where [servername] is the Windows hostname or fully-qualified domain name of the server. Connection is on TCP port 80 by default. The installer will create a SQL database called 'SecureAssessLocal' on the SQL server and will create a database user called 'secureassess'. The installer will create a service called 'SecureAssess Local Helper Service' on the host server.

Notes on the System Requirements

BTL recommends the use of a dedicated server. If this is not possible, all steps must be taken to ensure that maximum resources are available whilst exams are in progress.

Other running services or applications may adversely affect the performance of SecureAssess Local. This application should not be installed on a Domain Controller and the use of virtual machines should be avoided. To aid a smooth test delivery session, when running exams it is important to ensure that, wherever possible, network activity is kept to a minimum.

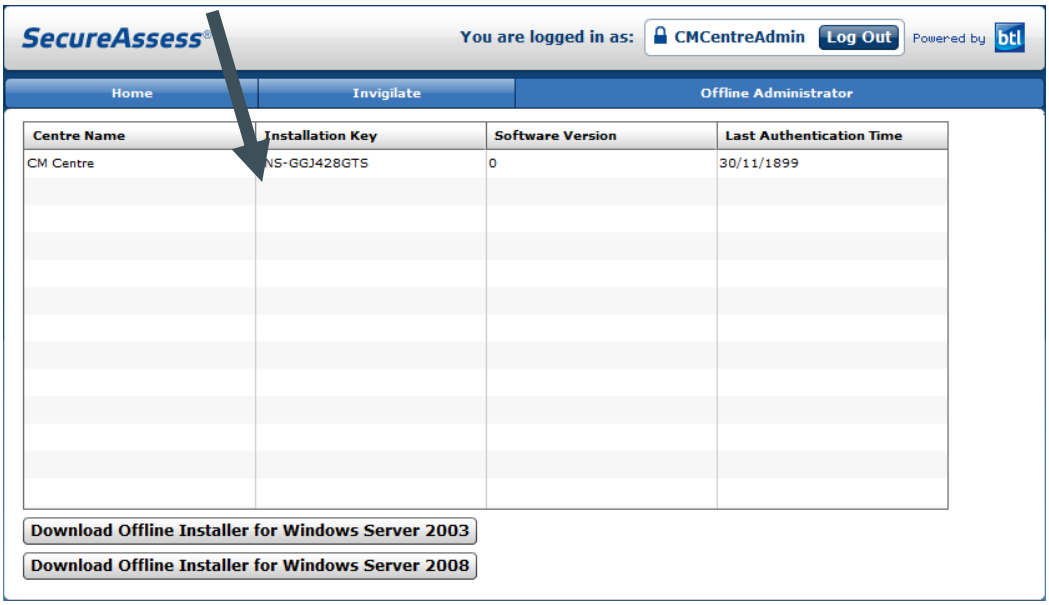
Installation

The installation process must be carried out by the SecureAssess Technical Contact for the centre; you will need to have login access/permissions as a Server Administrator, both for the SecureAssess system and for the server you will be installing SecureAssess Local onto.

Log into SecureAssess online (https://[organisation].secureassess.co.uk) and click on the "Offline Administrator" menu button.

If you do not have access to this, then you will need to contact BTL's Service Desk to ensure you are given the correct permission.

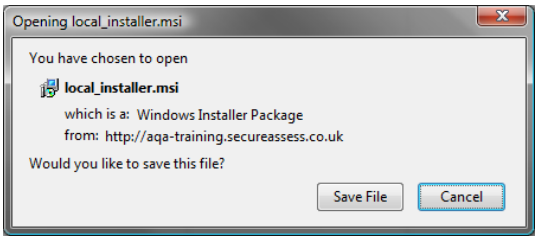
On the Offline Administrator tab you will see your centre name and the installation key. Make a note of your installation key.



The 'Download Offline Installer' button on this screen allows you to download the software needed to install SecureAssess Local on your server (the SecureAssess Local installer for either Windows Server 2003 or Windows Server 2008).

Click the button of whichever version of SecureAssess Local you wish to install. Clicking either of these buttons will display a dialogue box so you can save that installer file.

(Screenshot, right, was taken using Windows Vista and Mozilla Firefox.)



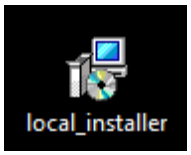
Create a folder called "SecureAssess Local" on the machine you will be installing SecureAssess Local on. Using this new folder, save the installer file (it's an MSI file) to your hard drive.

Note: If you get an error when trying to use the 'Save' function, then choose to 'Run' the file instead.

When you've downloaded the appropriate MSI file, locate it and run it.

Step by Step Guide to Installing SecureAssess Local

Double-click the SecureAssess Local Installer to start the Installation Wizard.

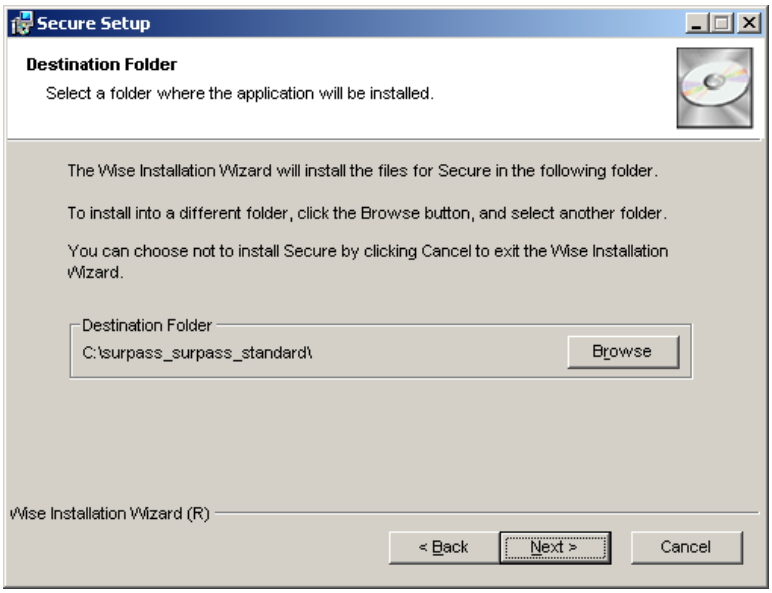


Step 1

Confirm that you have all the minimum requirements in place and click Next.

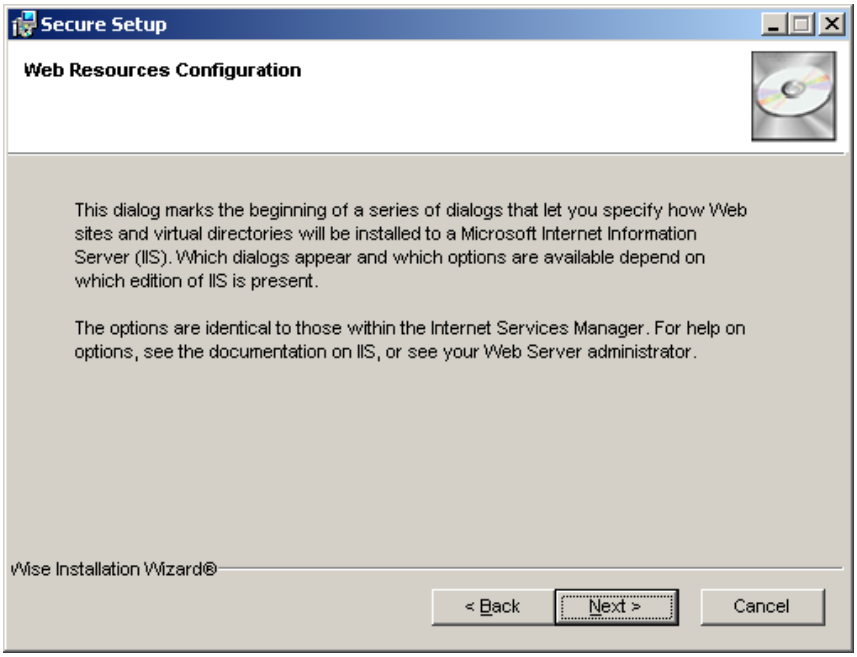
Step 2

This allows you to choose the location where the software will be installed. Once you're satisfied with the location, click Next.



Step 3

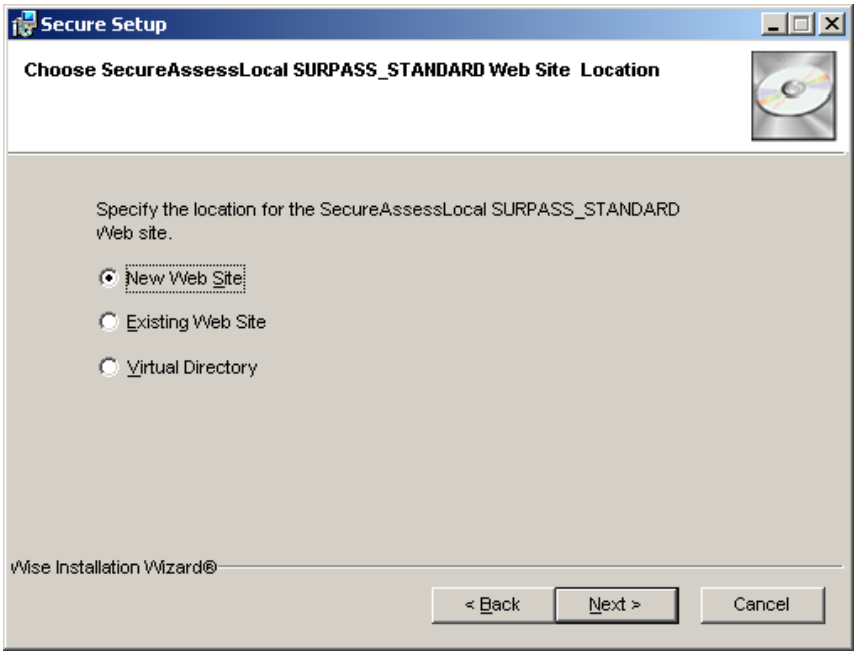
A screen will give you more information about the nature of the following steps.



Click “Next”.

Step 4

You will now be able to choose from 3 possible installation options.



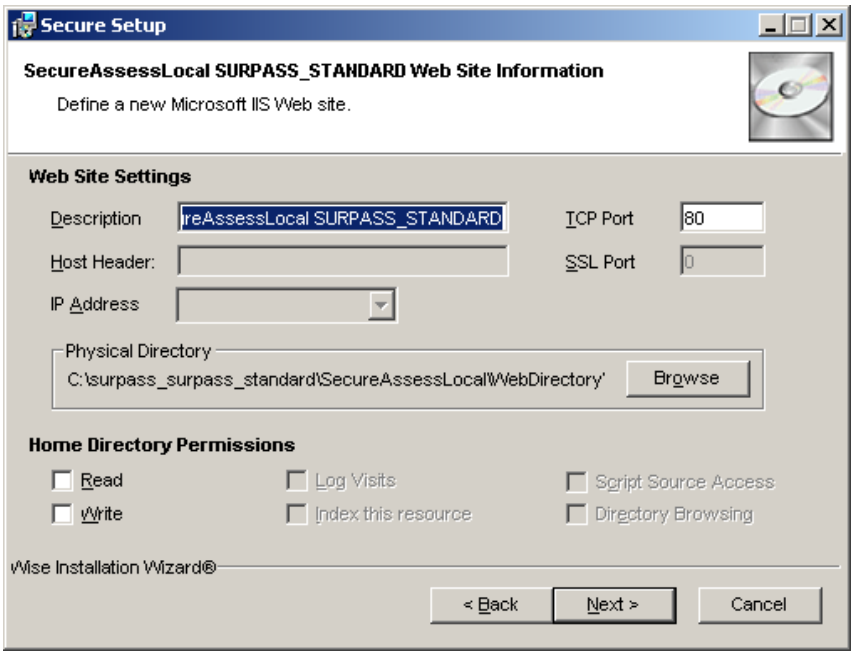
Select where you want to install SecureAssess Local and then click “Next”.

New Web Site

If you are creating a new IIS web site for SecureAssess Local then the following screen will be displayed.

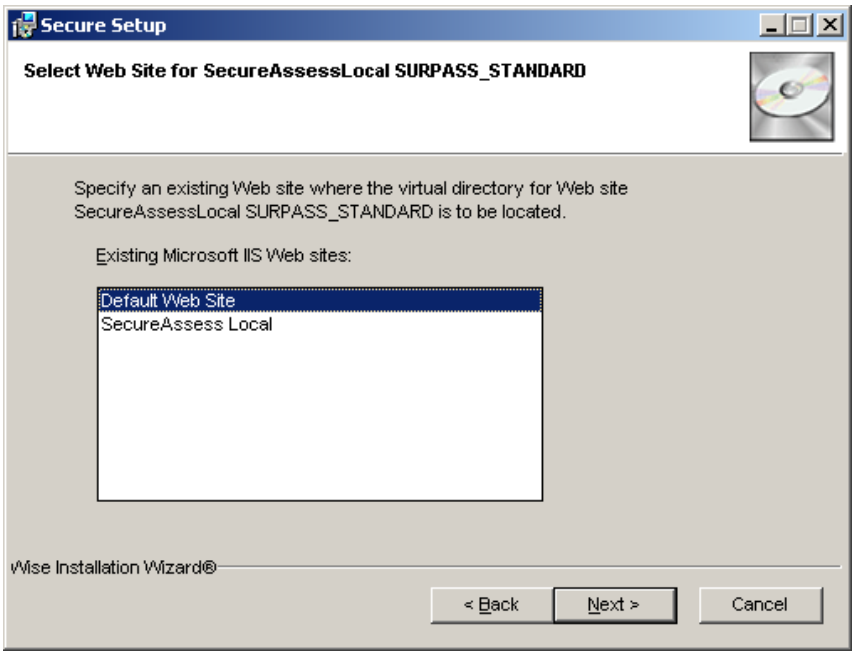
Enter a description for the website if you require a different one from the default.

Enter the port number to be used and tick the “Read” and “Write” permissions boxes.



Click “Next” to proceed.

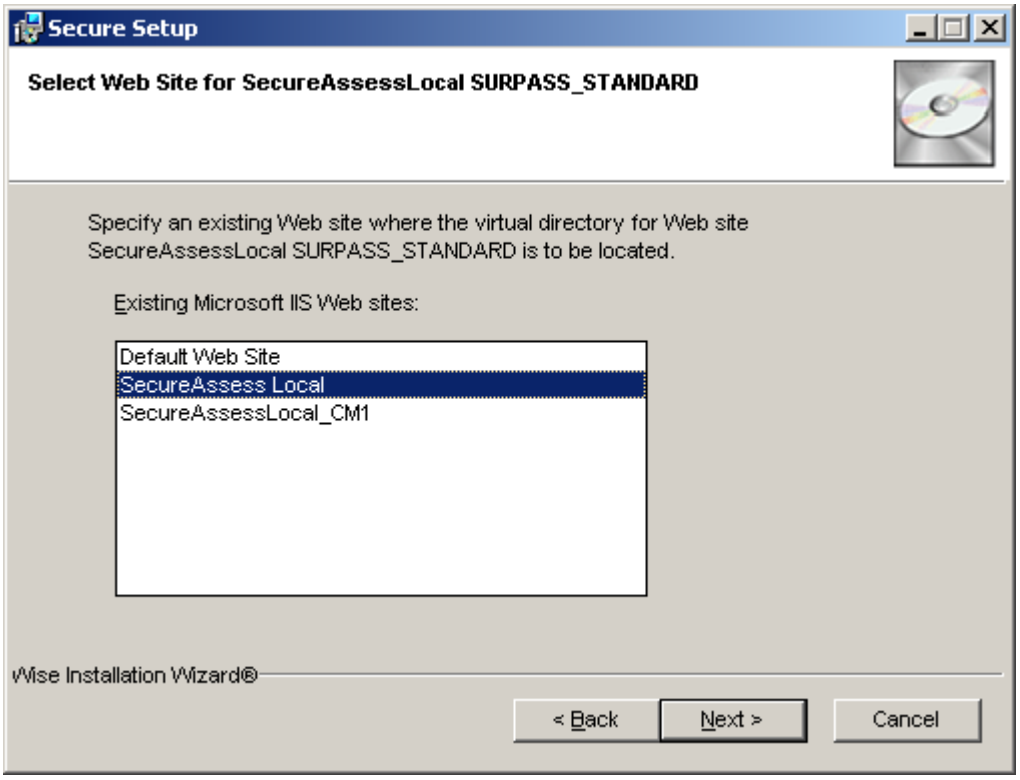
Now select an existing website where the new virtual directory will be created.



Click “Next” to proceed. Go to Step 5.

Existing Website

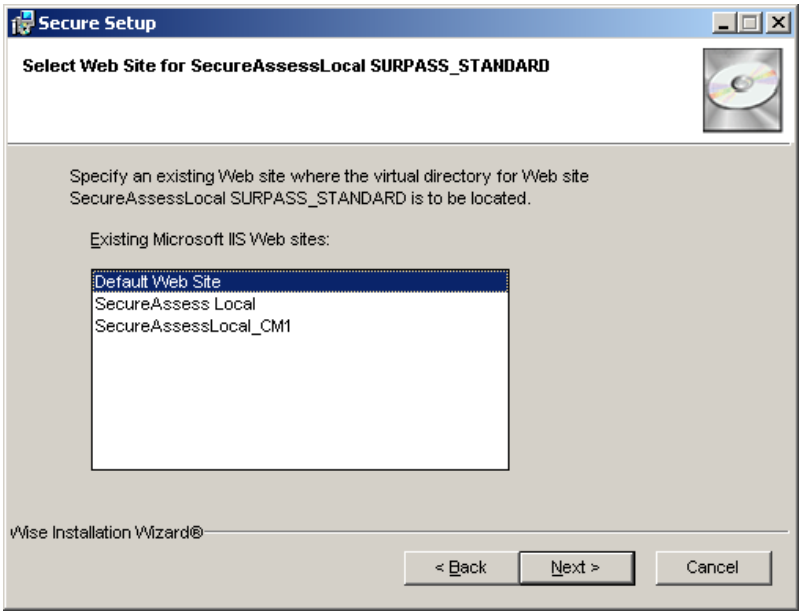
If you are installing to an existing website, select the website where you want to create the new directory.



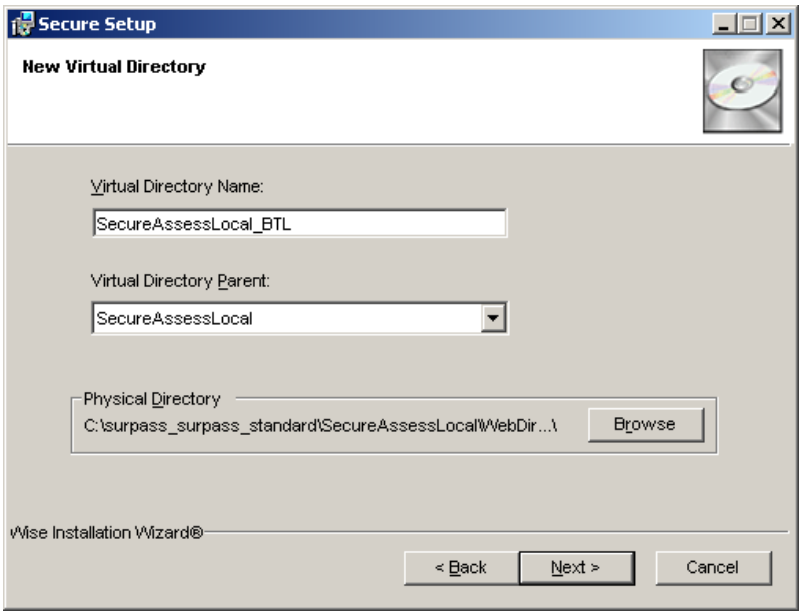
Click "Next" to proceed. Go to Step 5.

Virtual Directory

Select which website you wish to create the new virtual directory.



Enter a name for the new virtual directory and select the Parent Directory of the new virtual folder from the dropdown menu.



Click “Next” to proceed. Go to Step 5.

Step 5

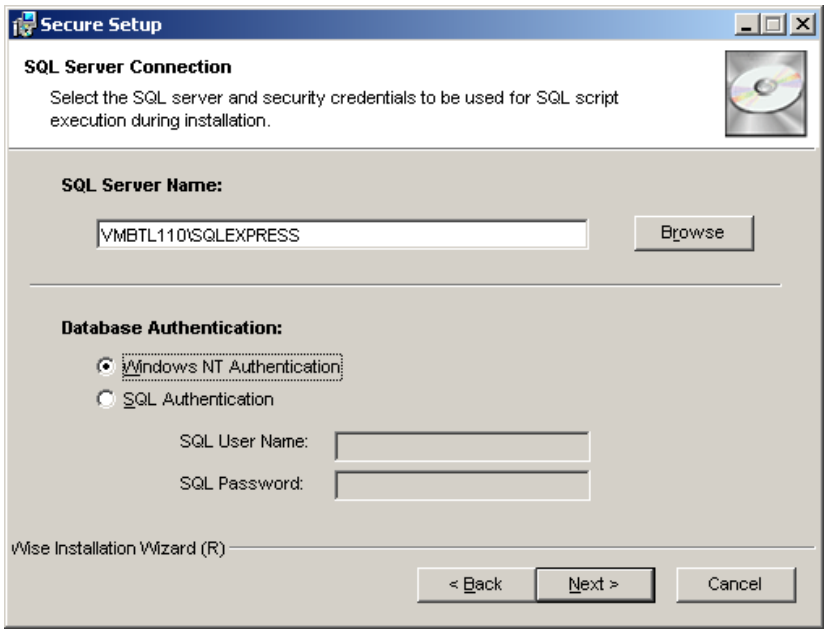
Specify the database server's Computer Name. If you are using SQLExpress installed on the same machine then typically the SQL server's Name will be:

machine_name\SQLExpress.

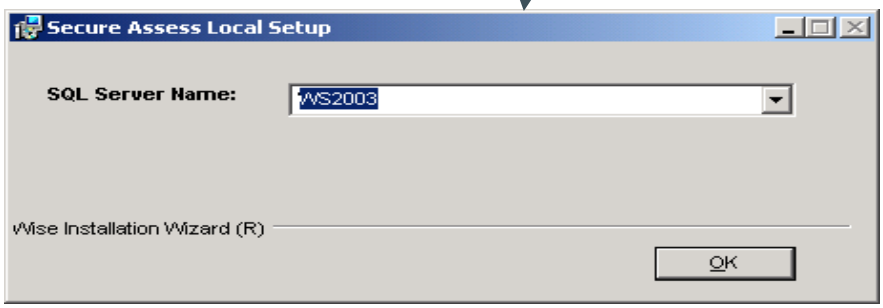
If the SQL Server is on the same machine then select 'Windows NT Authentication'. If the SQL Server is on a different machine and you are logged in as a Domain Administrator, or logged in with an account that has SYSADMIN rights on the SQL Server, then select 'Windows NT Authentication'.

It is essential that you ensure your SQL server has Mixed Mode Authentication switched on. Refer to Appendix 4 for more information on this.

If selecting SQL Authentication, provide the relevant SQL User Name and SQL password.



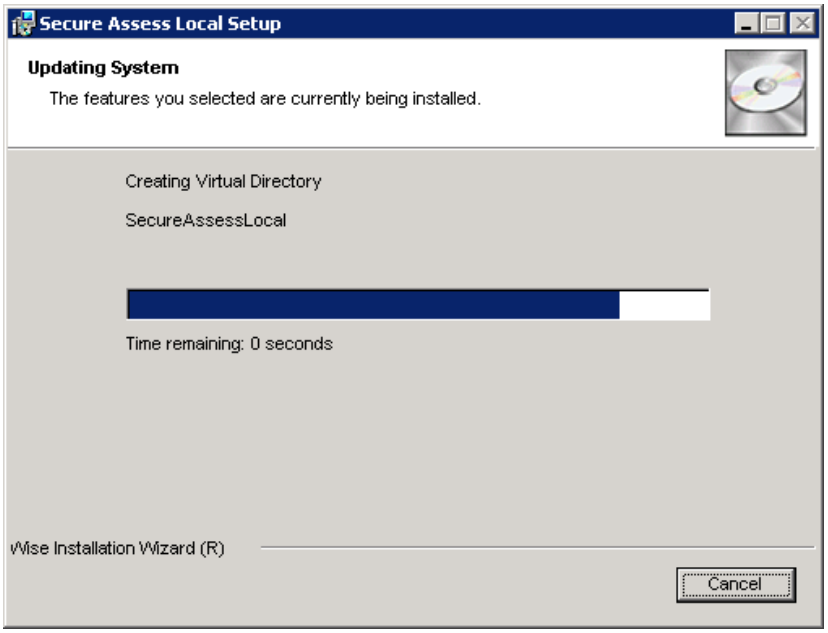
The Browse button can be used to display a dialogue box where you can locate a database instance.



Once you've selected the server you want to install SecureAssess Local on, click Next. This will test the database connection before proceeding.

Step 6

A progress bar will appear whilst the software is installed.



Step 7

Once the software has been installed you can click Finish.

The Configuration Wizard/Error 997

If the configuration Wizard doesn't display properly once you've installed SecureAssess Local, and you are shown an 'Error 997' message instead, then you'll need to check that ASP.NET and Active Server Pages are enabled ('Allowed') in IIS.

Follow the guidance given in Appendix 5 to enable Active Server Pages and configure the SecureAssess Local server to use ASP.NET v2.

Note: If this doesn't rectify the problem, or if these two items are already 'Allowed', then contact BTL's Service Desk.

Configuration Wizard

Once the software has been installed, launch Internet Explorer and navigate to your local SecureAssess site.

The default address for this will be of the form:

http://[servername]/secureassess.html

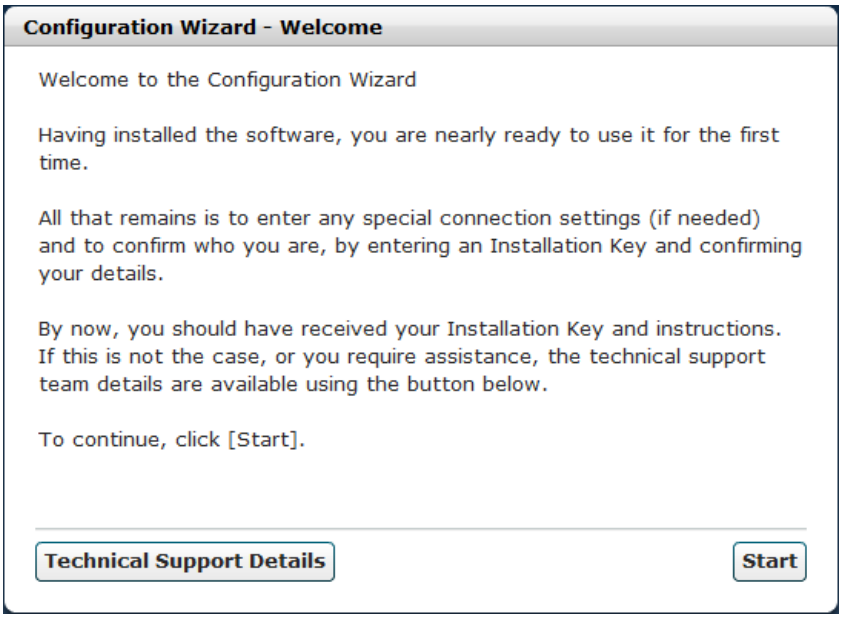
If you amended the default installation details, please look for this page at the equivalent location.

Note: You can access the same interface from any computer, with a web browser, on your network, provided that Flash Player 9 or 10 is installed on that machine.

This will display the first page of a configuration wizard. You may have to wait a short while for the Configuration Wizard to be displayed, please be patient. Once the Configuration Wizard welcome screen is displayed, click 'Start' to begin the configuration process.

Note: If the Configuration Wizard doesn't display, and you are shown 'Error 997' instead, please consult the information on the previous page regarding Error 997.

Step 1



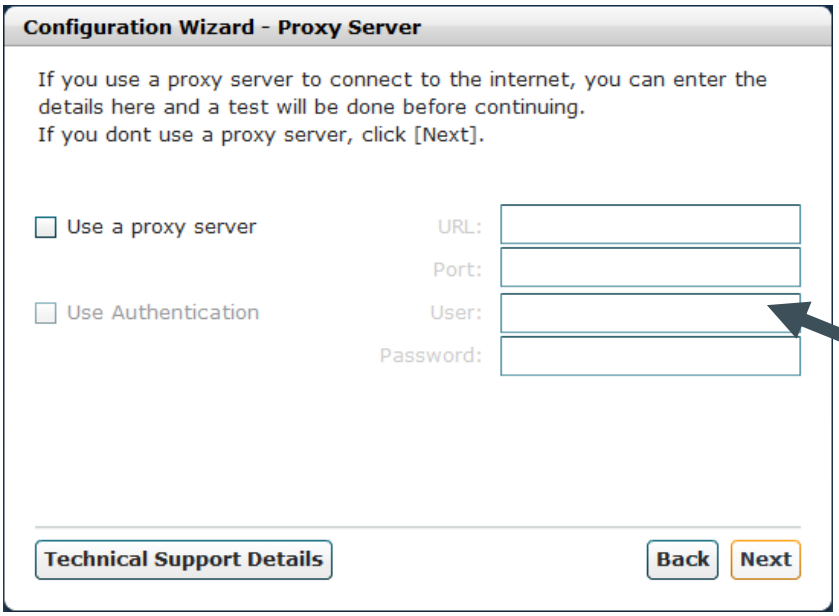
Clicking the Technical Support Details button at any stage of the Configuration Wizard will show you the BTL Service Desk contact details for assistance with the installation. If the awarding body are offering first line support then their technical team's details may be displayed instead.

Click Start to proceed with the Configuration Wizard.

Step 2

If proxy setup is required, then enter the details here and click Next.

You'll have to click the tick box to make the proxy fields become active so you can enter the details.



If you need to add 'Use Authentication' information here then please bear in mind that, if you're using multiple domains, you'll need to include Domain information as well as the User name.

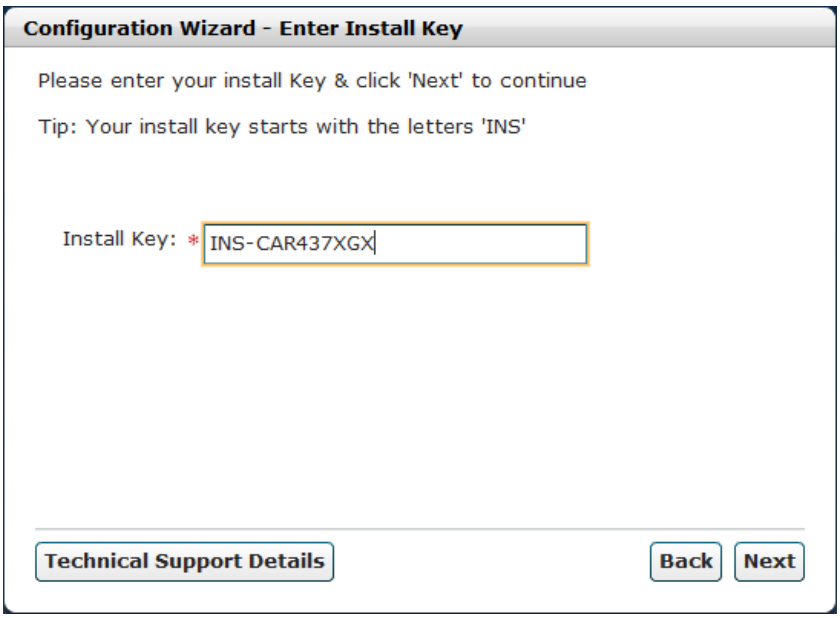
This means the information in the information you enter in the 'User' field will take the form:

DomainName/UserName

SecureAssess Local will connect through the proxy server to SecureAssess Central at the address: https://[organisation].secureassess.co.uk, using HTTPS and port 443.

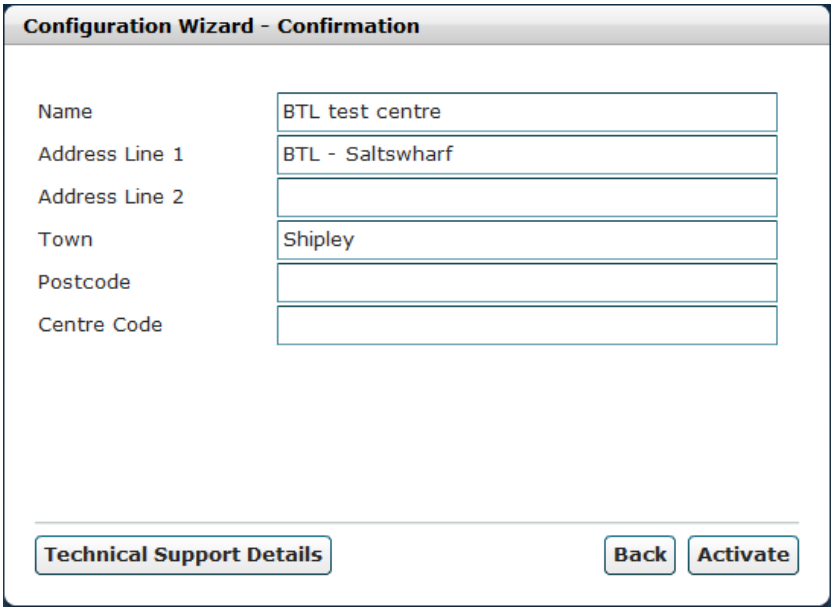
Step 3

Enter the installation key (as noted at the start of this chapter) and click Next.

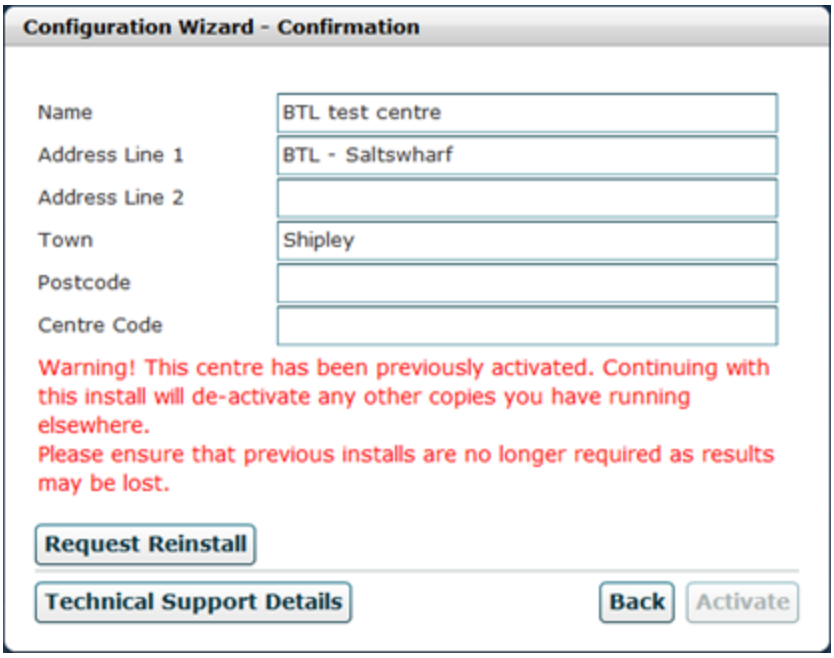


Step 4

The next screen will confirm the details for your centre.



If the installation key for your centre has been previously used (for example if you need to move the SecureAssess Local software to a new server) then you will be warned about this. Only a single instance of SecureAssess Local can be current per install key.



In order to confirm this action you must click Request Reinstall. This will then make the Activate button available. Alternatively, you can try refreshing the web page – this will sometimes fix this problem.

Click on the 'Activate' button to confirm and activate the SecureAssess Local system.

At this point, the SecureAssess Local Login screen will appear and you will be able to log in using the same username and password as you use to log into SecureAssess Central.

Note: If, after clicking Activate, the Login page doesn't appear, click on Activate again. A message may be displayed, informing you that SecureAssess Local appears to have been configured already. Close this message and refresh the browser window, the Login page will now appear.

Using SecureAssess Local

The screens that are available within SecureAssess Local are:

- Home Screen
- Invigilation
- Local Administrator

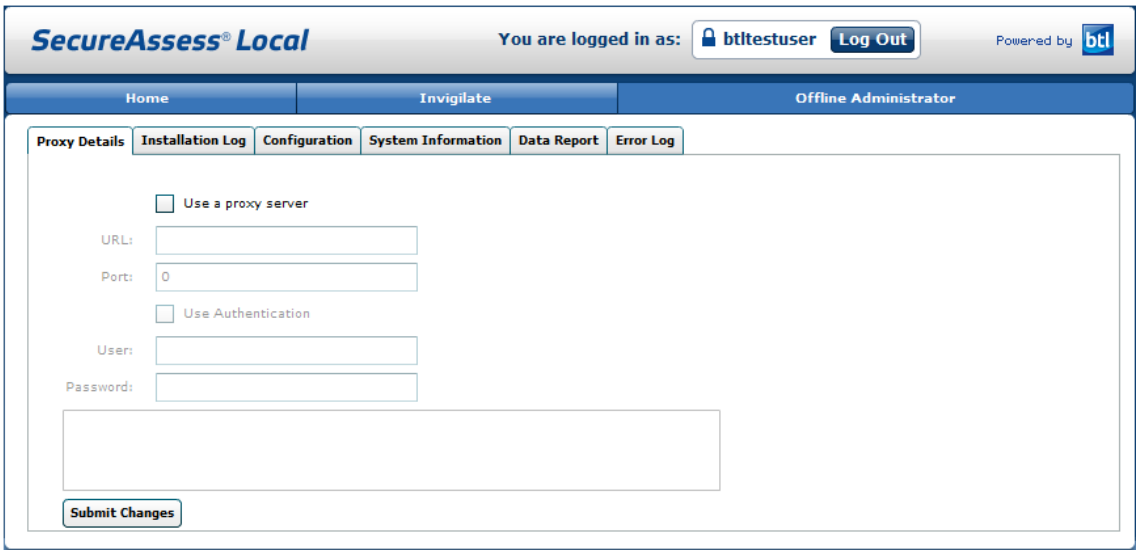
Depending on the Role assigned to you, you may not have access to the Invigilation or the Local Administrator screens. For details on Invigilation you should refer to the main SecureAssess Centre User Guide Document.

Offline Administrator

The Offline Administrator tab in SecureAssess Local offers six different tabs within it:

- Proxy Details
- Installation Log
- Configuration
- System Information
- Data Report
- Error Log

Proxy Details



The Proxy Details tab is initially selected when you open the Offline Administrator screen; using this tab you can view information on the proxy that SecureAssess Local has been configured to use.

If no proxy was chosen during the configuration process then the 'Use a proxy server' option won't be ticked, and the rest of the information will be greyed out.

If you need to enter the details of a proxy server then you can do so here. When you 'tick' the 'Use a proxy server' option, the rest of the fields will become active so you can insert the relevant information.

Remember, if you're using multiple domains, then you'll need to complete the 'User' field using the convention of DomanName/UserName.

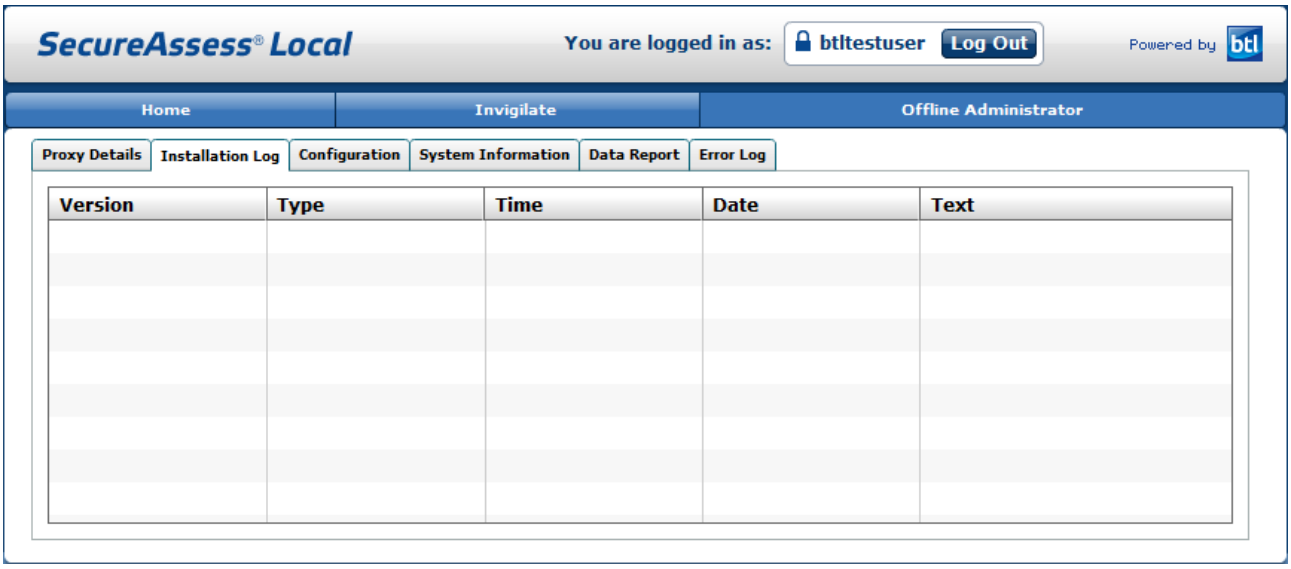
The same is true for the 'Use Authentication' options; the tickbox must be 'ticked' so you can enter information in the fields when they become active.

To confirm any changes you've made on this screen, click the 'Submit Changes' button.

Your centre may not make use of a proxy. If this is the case then you don't need to put any information in any of these fields.

Warning: you should only change these settings if you are certain and sure of what the implications are. Remember that any changes you make will affect all users of SecureAssess Local at your centre, not just you.

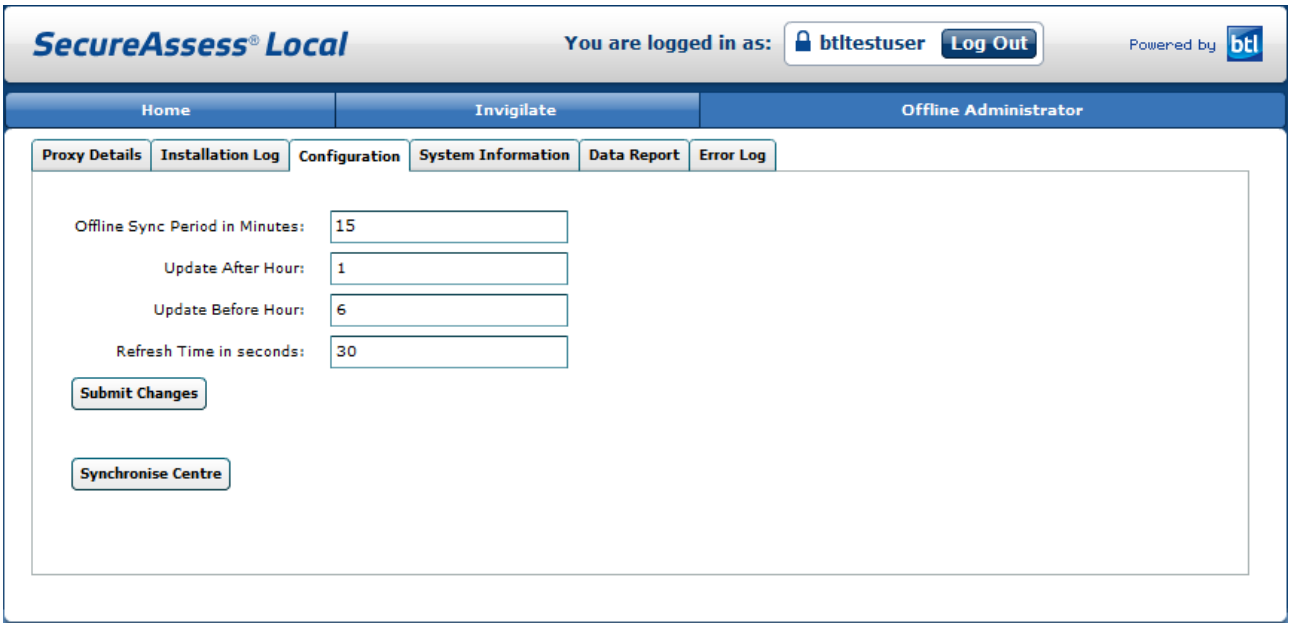
Installation Log



The Installation Log tab provides a table of information showing the types, times and dates of patches to the SecureAssess Local system. These patches are automatically 'pushed out' to your installation and applied without any need for action from you.

This table serves as information and reference only. There is nothing that you can interact with for this tab.

Configuration



The Configuration tab is where you control how SecureAssess Local behaves and how it interacts with SecureAssess Central. You can click into each field and amend any information as you please.

Offline Sync Period in Minutes	**How often the SecureAssess Local system will download newly scheduled exams from SecureAssess Central, and also upload the results of any completed exams.**
Update After Hour	**The time of day after which SecureAssess Local can check for, download and apply system updates, such as patches.**
Update Before Hour	**The time of day before which SecureAssess Local can check for, download and apply system updates, such as patches.**
Refresh Time in seconds	**How often the Invigilate screen will check for updated information on exams that have been downloaded or are in progress.**

When you are satisfied with changes you have made, click 'Submit Changes' button to confirm them.

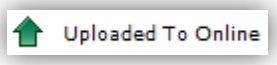
Synchronise Centre

The Configuration tab also offers a 'Synchronise Centre' button.

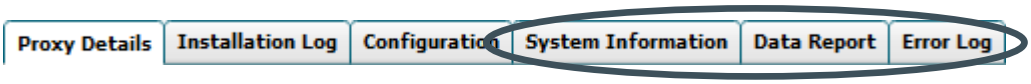
Use this button to force SecureAssess Local to synchronise with SecureAssess Central (check for any exams that are ready to be downloaded and upload any results from finished exams).

This overrides the 'Offline Sync Period in Minutes' property so you can check for any exams that need downloading from or uploading to SecureAssess Central there and then.

Any exams that the synchronisation process picks up will appear in the Invigilate table in the Invigilate tab screen. Simultaneously, any exams that are waiting to be uploaded to SecureAssess Central will be uploaded, and then the icon in their status column in the Invigilate screen will change to a green, upwards-pointing arrow (see image below) – showing they have been uploaded successfully to SecureAssess online.



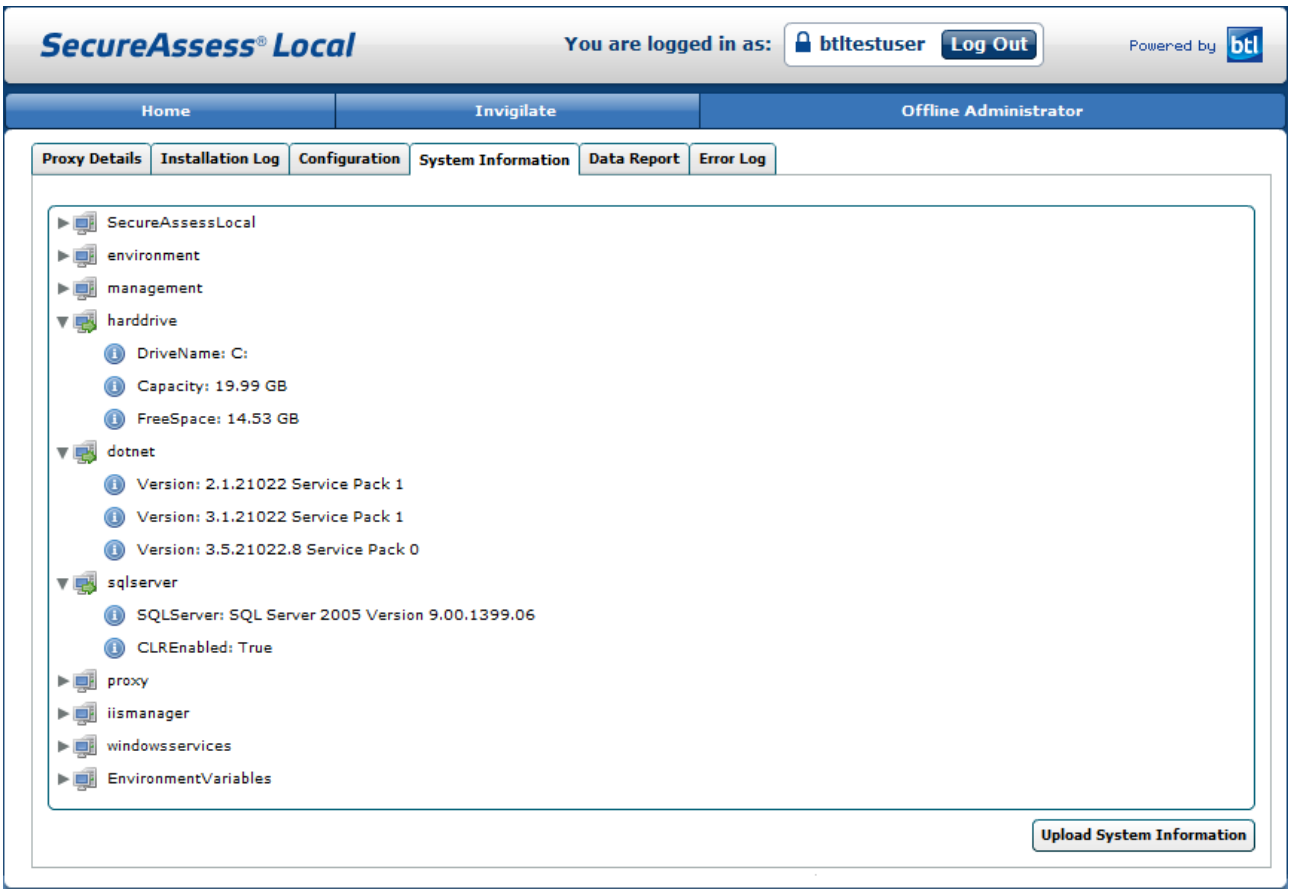
System Information, Data Report and Error Log tabs



These three tabs are used to display information from the server that SecureAssess Local is installed on, including hardware specifications and software version information. From these screens you can also upload a snapshot of this information, which will help the BTL Service desk troubleshoot any problems you might encounter.

System Information

The System Information screen will display information about the server that SecureAssess Local is installed on. There are a series of headings that you can expand by clicking the arrow next to each heading: this will expand the heading and show the details of the server.



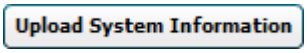
The headings are as follows:

- SecureAssessLocal: Information about the SecureAssess Local installation, including software version.
- environment: Details of the server name, Operating System & service packs, etc.
- management: Further information on the server type and Memory.
- harddrive: Details on the storage drive name, capacity and available space.
- dotnet: Information on the versions of Microsoft .NET Framework installed & any service packs.
- sqlserver: SQL Server version details.

- proxy: Details of any configured proxy server(s).
- Iismanager: Information on IIS and the websites configured on the server.
- windowsservices: Details of the services, running or stopped, on the server.
- EnvironmentVariables: Extra miscellaneous information.

Note: Don't worry if you don't understand everything detailed here as this functionality is mainly to allow the BTL Service Desk team to effectively help you troubleshoot any problems.

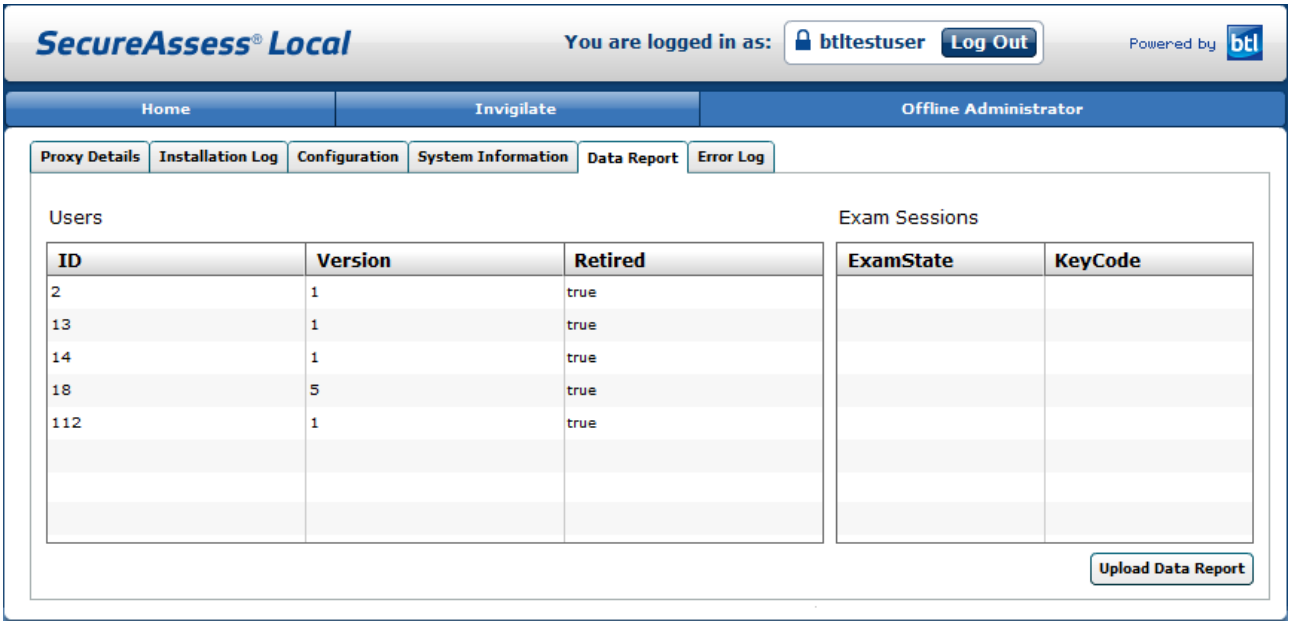
To upload the information from this screen to SecureAssess Central, click the 'Upload System Information' button.



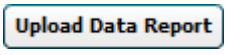
Data Report

Clicking the Data Report tab displays a screen with two tables on it:

- Users table: this table displays information about all users of the SecureAssess Local system.
- Exam Sessions table: this table lists all exam KeyCodes and their current ExamStates.



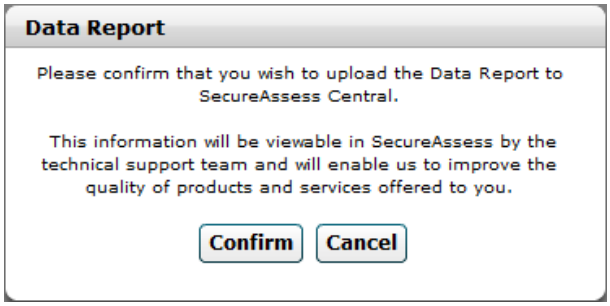
You can click the 'Upload Data Report' button to upload the information from this screen to the SecureAssess central system. This button is located in the bottom-right corner of the SecureAssess Local interface.



When you click this button, a pop-up will be displayed, asking you to confirm you want to upload the data to SecureAssess central.

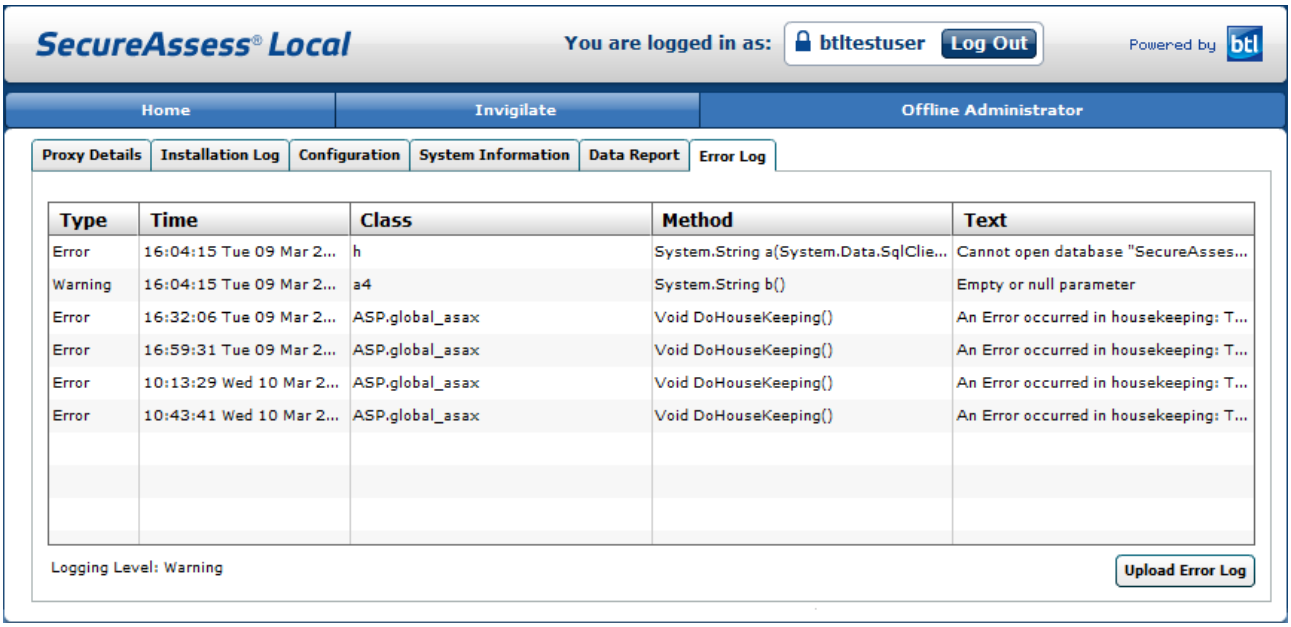
To confirm this and continue with the upload, click 'Confirm'.

Click 'Cancel' to close the pop-up and continue without uploading the data.

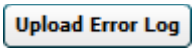


Error Log

On the Error Log screen, there is a table that shows information on all errors that have been reported in the SecureAssess system on the server.



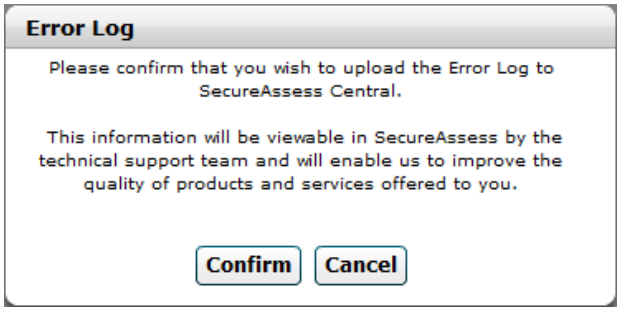
You can click the 'Upload Error Log' button to upload the information from this screen to the SecureAssess central system. This button is located in the bottom-right corner of the SecureAssess Local interface.



When you click this button, a pop-up will be displayed, asking you to confirm you want to upload the data to SecureAssess central.

To confirm this and continue with the upload, click 'Confirm'.

Click 'Cancel' to close the pop-up and continue without uploading the data.



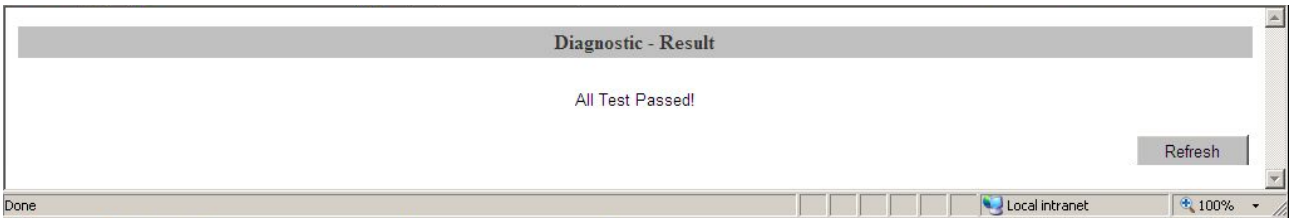
Appendix 1: Diagnostics Page

In the event that there are issues with the SecureAssess Local installation, a diagnostics page is available at:

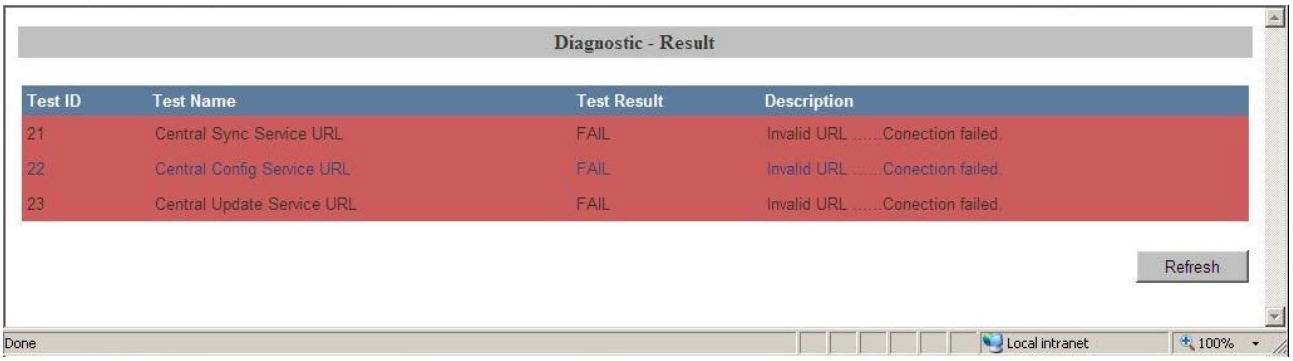
http://[servername]/secureassesslocal/showdiagnostic.aspx

If you amended the default installation details, please look for this page at the equivalent location.

This will display the status of the system checks. If no errors are found then a page will be displayed like below:



If any of the checks fail, then they will be listed, like in the image below:



You can provide details of any 'FAIL' items when contacting the BTL Service Desk.

Appendix 2: Installing Microsoft Internet Information Services (IIS) 6.0

You should install IIS first if possible i.e. before installing the .NET framework or SQL Server 2005 Express Edition.

Installing IIS

Important: Before you begin attempting to install IIS 6.0, please be aware that you may need the Windows Server Installation Disk to carry out the install.

To install Microsoft Internet Information Services (IIS) 6.0:

1. Click Start > Control Panel.
2. Within Control Panel, double click 'Add or Remove Programs'.
3. Click on 'Add/Remove Windows Components'.
4. Select 'Application Server'.
5. Click Next.

   Note: Here you may be prompted to insert/locate the Windows Server Installation Disk

6. The wizard will automatically install IIS.
7. Once the wizard has completed installation, click 'Finish'.

Appendix 3: Installing .NET Framework

A note on IIS and .NET

You should install IIS before installing the .NET framework if possible because when you perform the .NET setup, it configures IIS to recognise all the correct file types (such as .aspx). If you install the .NET runtime before IIS, you'll run into problems as IIS won't recognise your ASP.NET files and won't hand them off to the ASP.NET worker process to execute your code.

To solve this problem you can repair your IIS file mappings. You can do this by running the aspnet_regiis.exe command-line utility with the –i command-line parameter (for install), as shown here:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis.exe –i

At this point, ASP.NET will check your virtual directories and register the ASP.NET file types.

You don't have to perform this repair process if you install IIS first, and then install .NET.

The install procedure for the .NET framework

You should download the .NET framework from Microsoft's website. The minimum requirement for SecureAssess Local is .NET 2.0 plus the latest Service Pack (i.e. 2 or later), though there are further versions available.

The .NET 2.0 Framework installer can be downloaded from:

http://msdn.microsoft.com/en-us/netframework/aa731542.aspx

When you have downloaded the .NET executable file, you should double-click it to run it.

There are no non-default options you need to configure in order to make SecureAssess Local function as it should. Click through the steps of the installation wizard to complete the process.

You should restart the machine after successfully installing the .NET Framework.

NOTE: You should ensure that if you are running exams with .NET 2.0 installed, you should ensure that it has at least Service Pack 2.

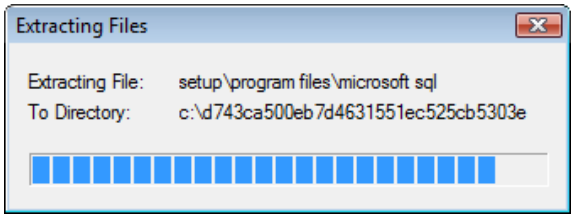
Appendix 4: Installing SQL Server 2005 Express Edition

You should download SQL Server 2005 Express Edition from Microsoft's website:

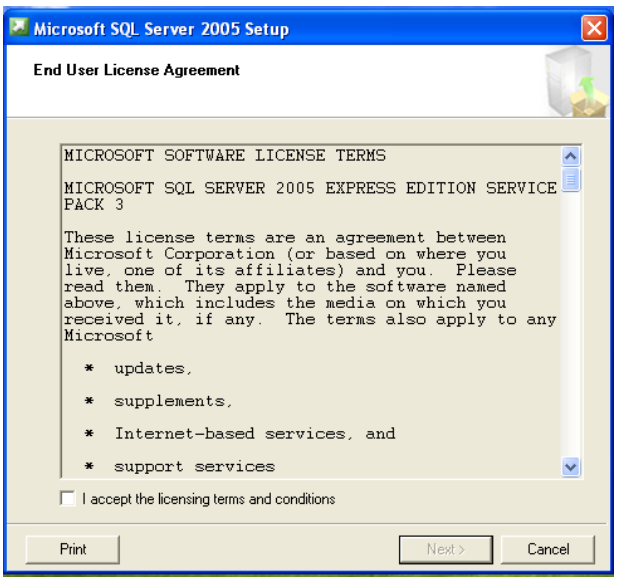
http://www.microsoft.com/express/sql/previous/default.aspx

When you've downloaded the file, double-click it to run the installer.

As shown below, the installer will extract files to a temporary location...



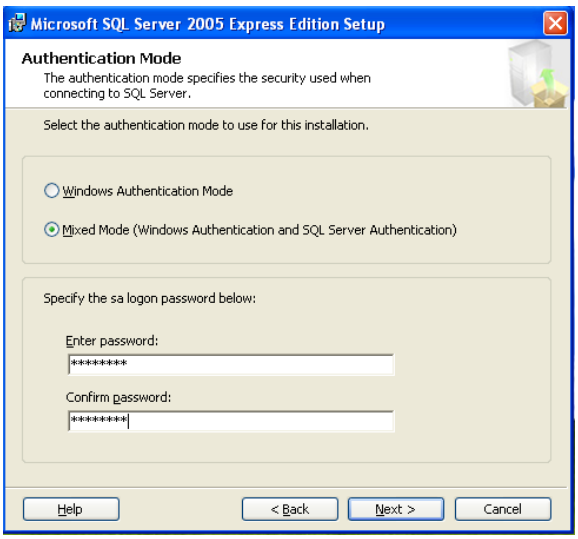
...and then initialise the installation wizard.



You should accept the EULA and click 'Next'. On the following screens you can confirm and click through the wizard to confirm the default options - with the exception of the Authentication Mode screen.

Mixed Mode Authentication

When you reach the Authentication Mode stage of the installation wizard, you need to make sure that 'Mixed Mode (Windows Authentication and SQL Server Authentication)' is selected.



You can now proceed with the install as usual confirming default settings.

If you already have SQL Server 2005 Express Edition installed but don't have Mixed Mode Authentication enabled, you can change this using the following method.

Enabling Mixed Mode Authentication on an existing installation of SQL Server 2005 Express Edition

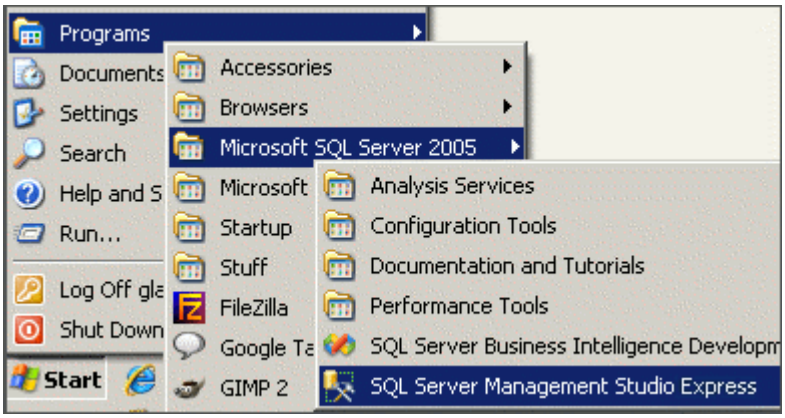
The following steps require you to install Microsoft SQL Server Management Studio Express.

You can download Microsoft SQL Server Management Studio Express from the following location:

http://www.microsoft.com/downloadS/details.aspx?familyid=C243A5AE-4BD1-4E3D-94B8-5A0F62BF7796&displaylang=en

If you've already got SQL Server 2005 Express Edition installed, but don't have Mixed Mode Authentication switched on, you can do this through SQL Server Management Studio or SQL Server Management Studio Express.

1. Click Start > Programs > Microsoft SQL Server 2005 > SQL Server Management Studio/ SQL Server Management Studio Express (depending on your version of SQL Server).



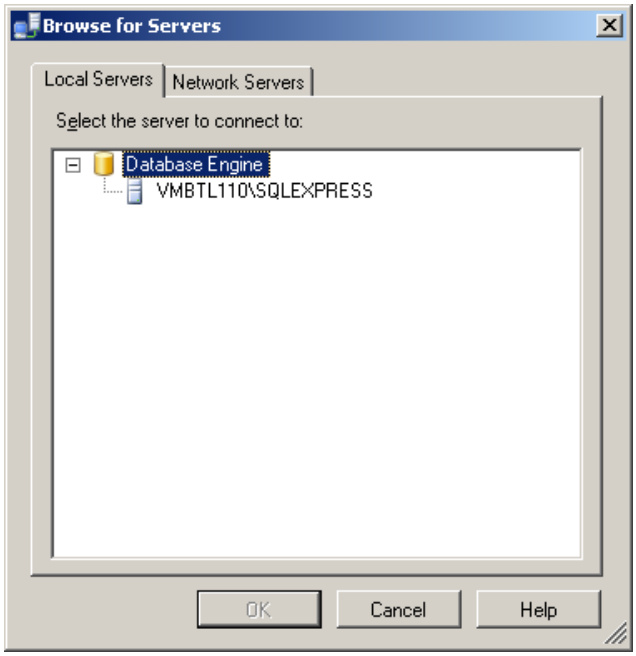
2. Enter the information you're prompted for:

    1. Server Type: Select Database Engine.
    2. Server Name: Enter the name or IP of the server where the SQL database is.*
    3. Authentication: select Windows Authentication.

he name of the server may
eady be present in the Server
me field. If it is not, and you
n't know the server name or IP,
u may be able to select it from
e dropdown list of servers that
ve been connected to before
ing this install of SQL Server
anagement Studio.

If the server has not been connected to using this install of SQL Server Management Studio before, then you will have to manually locate it. To do this, select Browse for more... from the dropdown list.

You will now be able to expand the Database Engine element explorer tree structure and locate the server you wish to connect to. You should only be looking for the server under the Local Servers tab, not the Network Servers tab.



Bear in mind that the server name to look for will be the name of the machine it is installed on (if all the default options were accepted when performing the install).

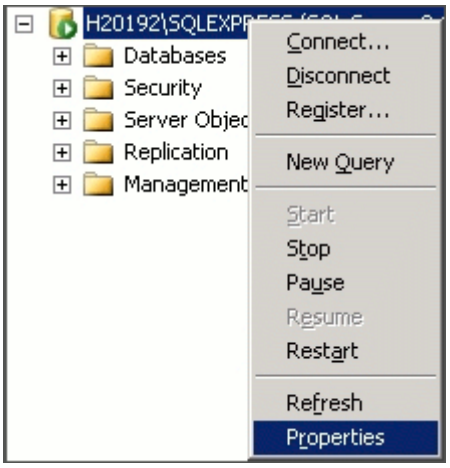
When you've located the server, click it to select it and then click OK.

The Browse for Servers dialogue will close and the server name will be displayed in the Connect menu.

Note: if the server you're looking for isn't displayed here then you need to contact your system administrator as the server, or relevant service, may not be running.

4. When you have entered all the correct details, click Connect.

5. Right-click the server name and select Properties from the context menu displayed.

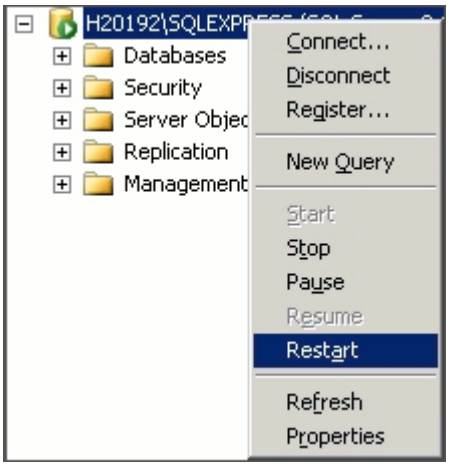


6. Select Security from the list on the left-hand side of the Server Properties menu.

7. Under the Server authentication heading, select SQL Server and Windows Authentication Mode.

8. Click 'OK'.

9. Right-click the server name and select Restart from the context menu displayed.



10. Wait a few moments for the service to restart before proceeding.

11. This completes the process of switching on Mixed Mode Authentication for this server.

Appendix 5: Enabling ASP.NET & Active Server Pages

You need to make sure these two items are enabled in IIS, after you've installed SecureAssess Local, in order for it to work properly. You also need to ensure that SecureAssess Local website is configured to use ASP.NET v2 in IIS.

By default, in IIS 6.0, ASP.NET and Active Server Pages are disabled: here's how to enable them.

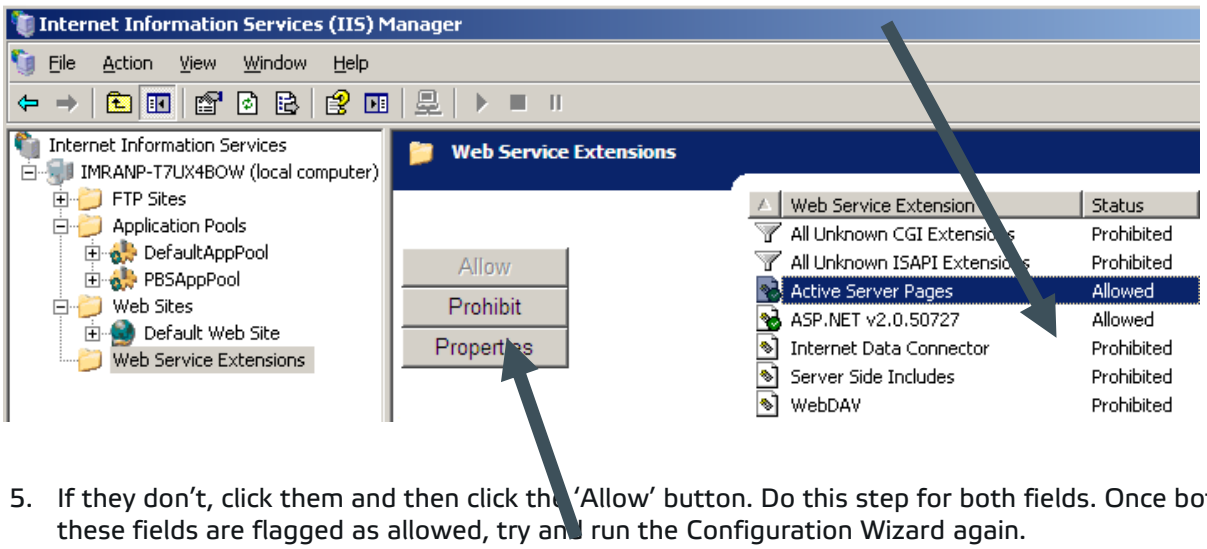
1. Click Start > Administrative Tools > Internet Information Services (IIS) Manager.

   Note: if Administrative Tools is not available from the Start Menu then you can access it by opening the Control Panel and then double-clicking the Administrative Tools icon there.

2. Click the + next to the server name to expand it (in the left-side panel).

3. Click the Web Service Extensions folder.

4. Check to see if ASP.NET and Active Server Pages have the word "Allowed" next to them, in the Status column.



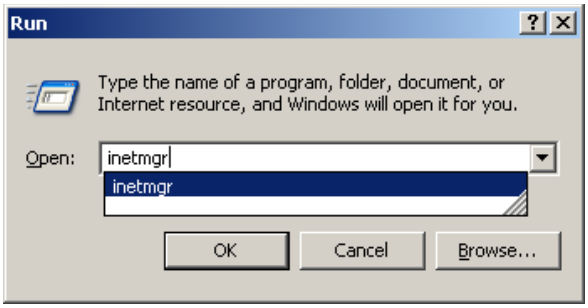
5. If they don't, click them and then click the 'Allow' button. Do this step for both fields. Once both of these fields are flagged as allowed, try and run the Configuration Wizard again.

Appendix 6: Configuring SecureAssess Local to operate on a new website

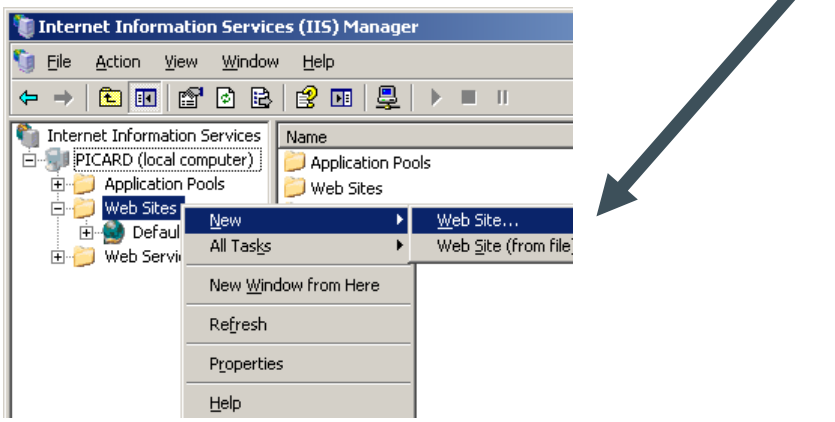
This may be necessary if the Default Web Site is in the 'Stopped' status and impossible to start. At the end of this process, it will be necessary to modify the Web Site's configuration files. The steps to complete this process are shown in Appendix 7.

Create New Website/Virtual Directory

Start IIS Manager by going to Start > Run and then running "intemgr".



In IIS Manager Right-click on the Web Sites folder, select 'New' and then 'Web Site' from the displayed context menus.

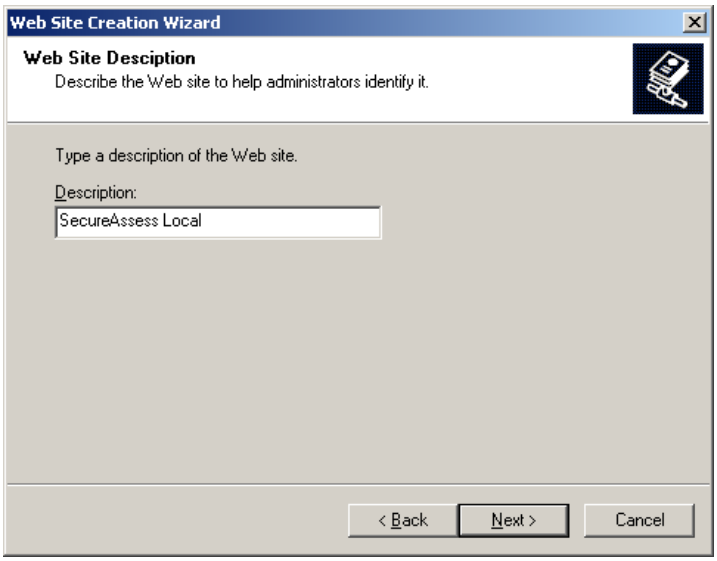


The Web Site Creation Wizard

The Web Site Creation Wizard will be displayed.

Click 'Next' to begin.

Enter a description of what this website is. In this example, it's called: "SecureAssess Local"



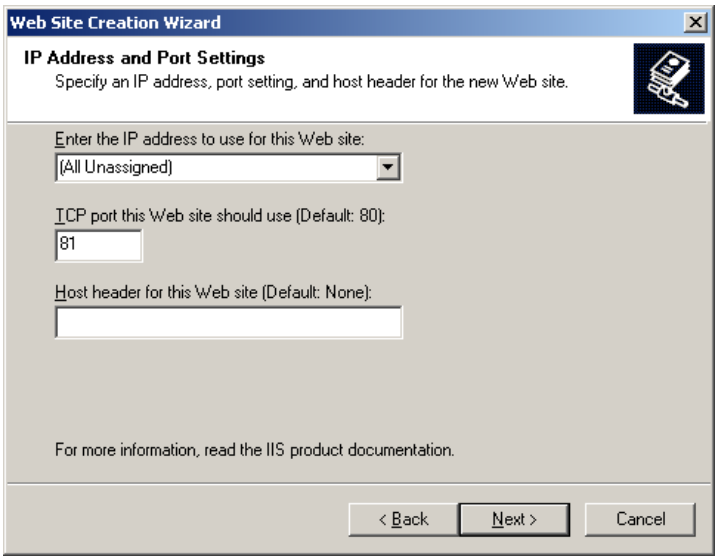
When you've entered this description click 'Next'.

Now enter the port number for this website to use.

In the example, port 81 has been chosen.

You can leave the IP address as “All Unassigned”.

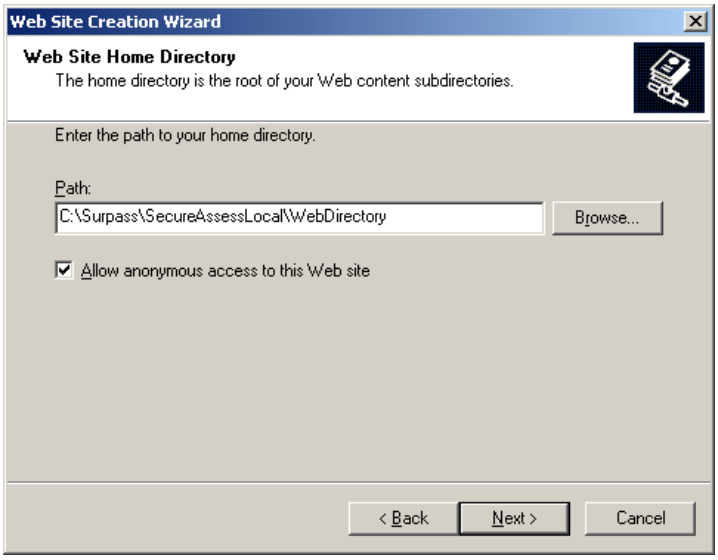
Click ‘Next’ to proceed to the next step of the wizard.



Enter the path of the SecureAssess Local “WebDirectory” folder.

Use the Browse function if necessary to help locate the folder.

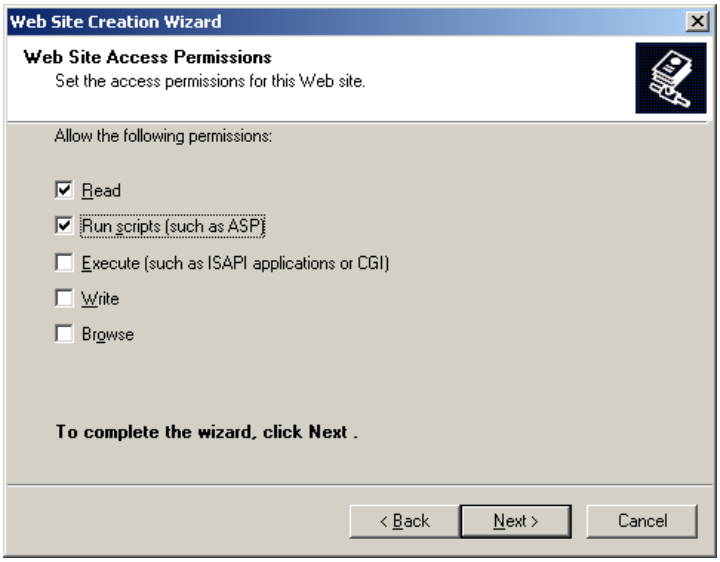
Click ‘Next’ when you’ve entered the path.



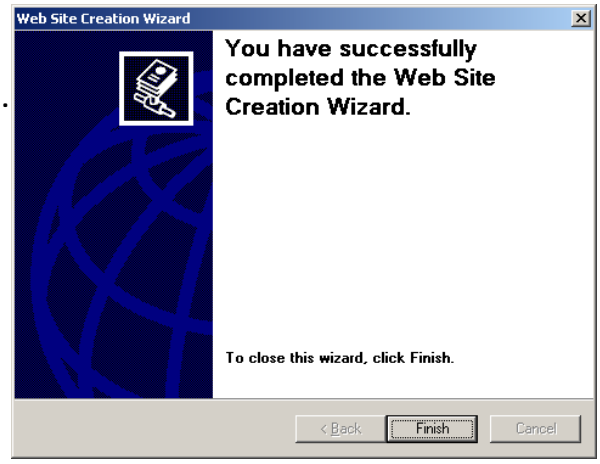
Now, leave all the options as they are, except for the “run scripts (such as ASP)” option.

Make sure this option is ticked.

When you’ve done this click ‘Next’ to proceed.

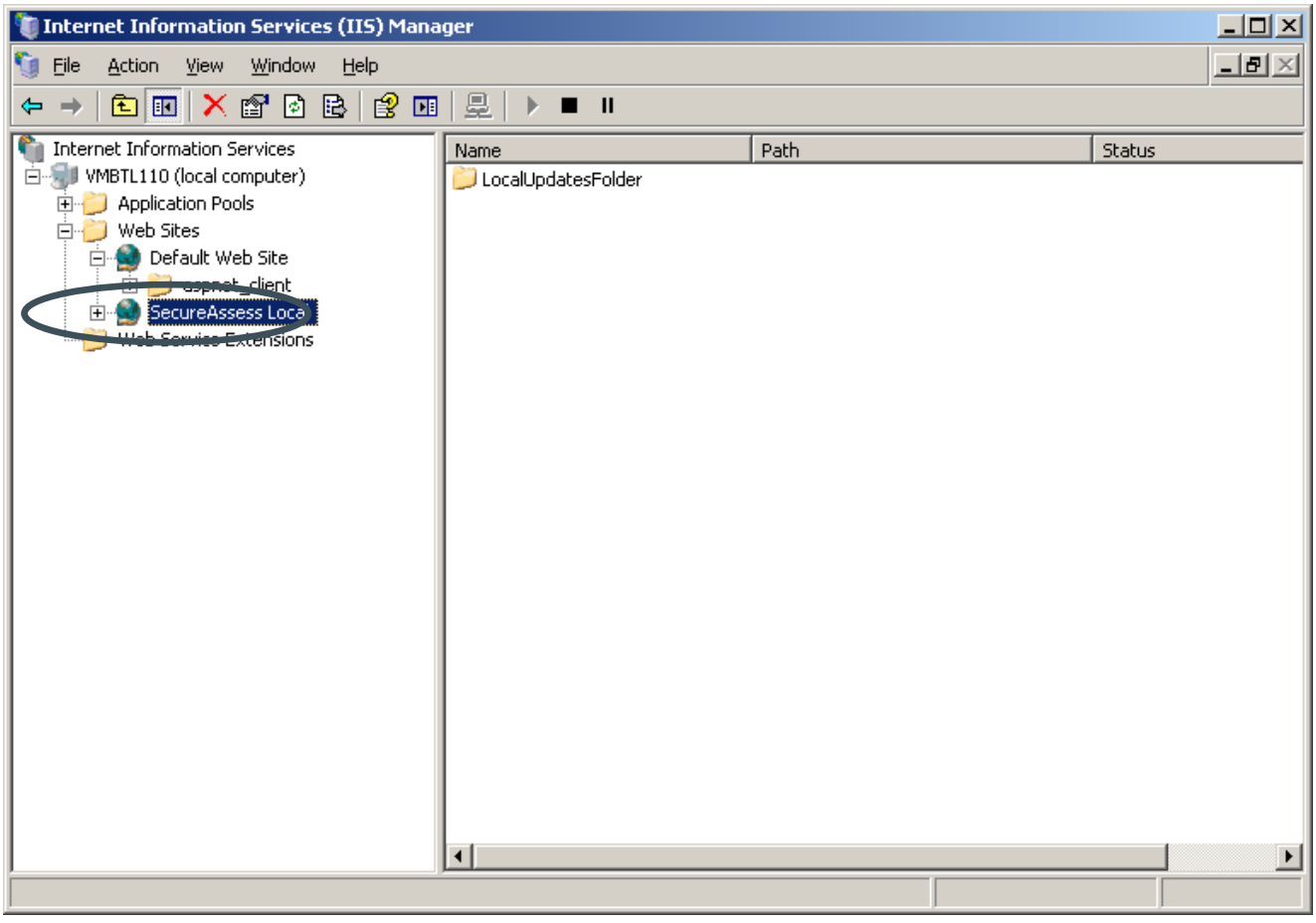


The finish page of the wizard will now be displayed.



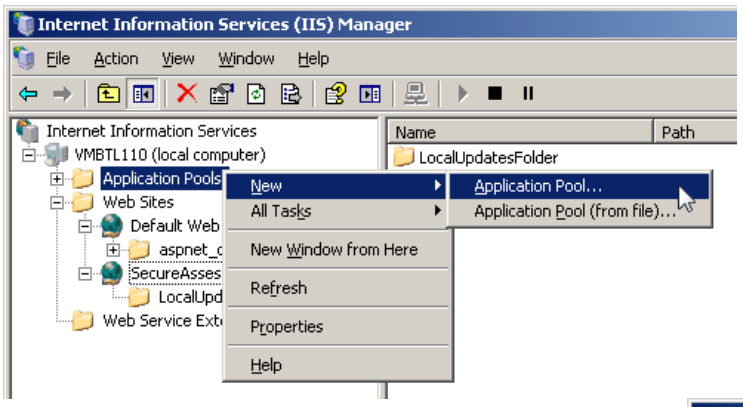
Click 'Finish' to exit the wizard.

The new website will be displayed in the list in the left panel of IIS Manager.



Create a New Application Pool

Create a new Application Pool by right-clicking the Application Pools folder in the tree structure in the left panel of IIS Manager and then selecting New > Application Pool.

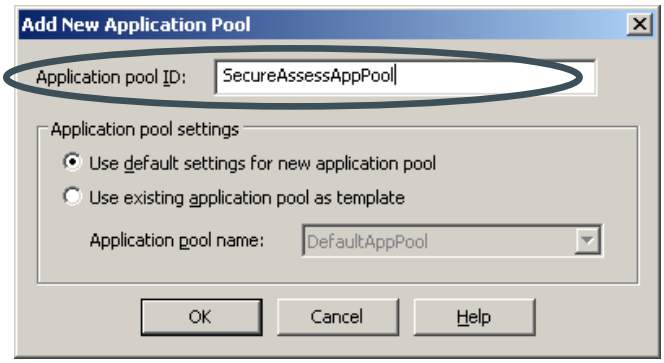


The Add New Application Pool dialogue will now be displayed.

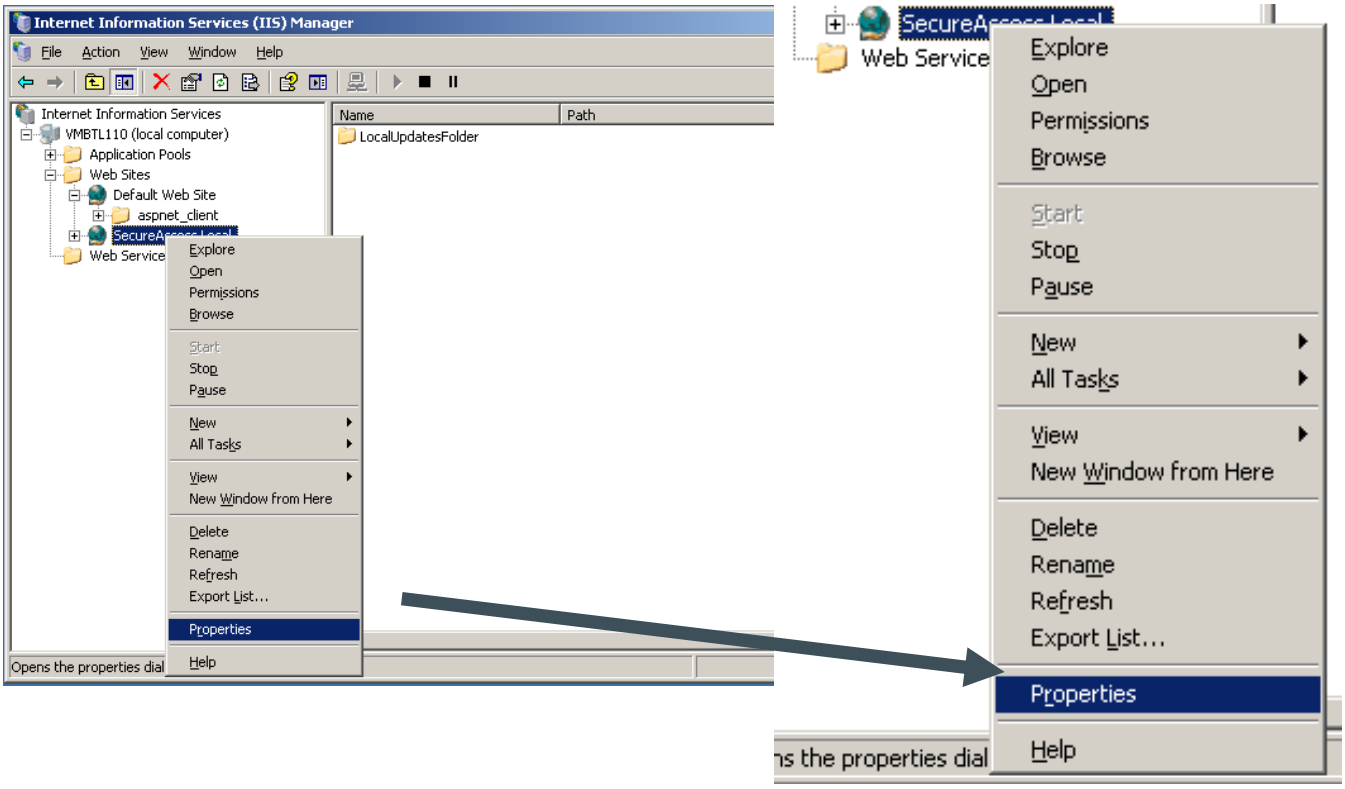
Enter the Application pool ID:

SecureAssessAppPool

Leave the Application pool settings as they are and click 'OK'



The new Application Pool will be shown in the tree structure in IIS Manager.



Set the Properties of the Website to use the new Application Pool

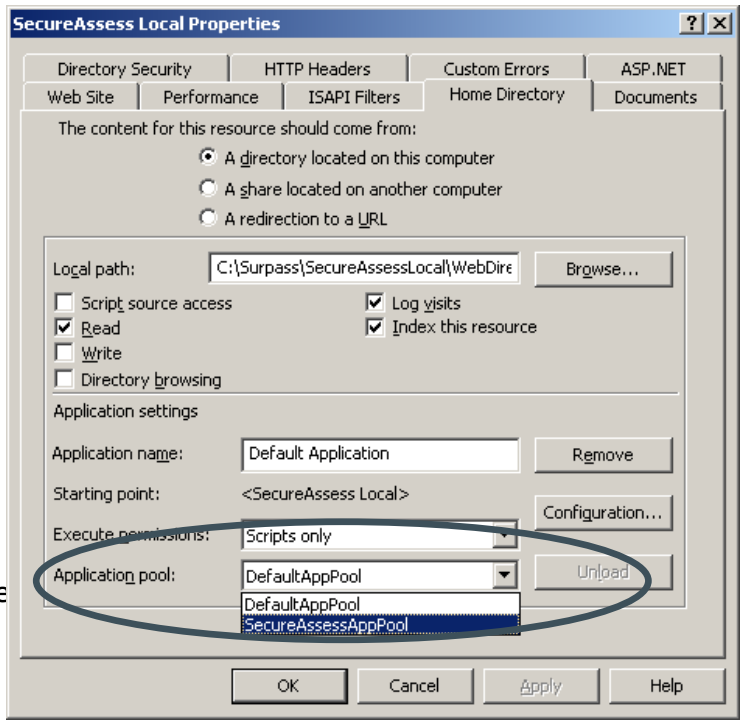
You now need to change the properties of the new website.

To do this, right-click the website in the left panel of IIS Manager and then select Properties from the displayed context menu.

Click the Home Directory tab in the SecureAssess Local website properties.

Now click the dropdown menu for the Application Pool field and select the SecureAssessAppPool pool you created.

Click 'Apply' to confirm the operation.



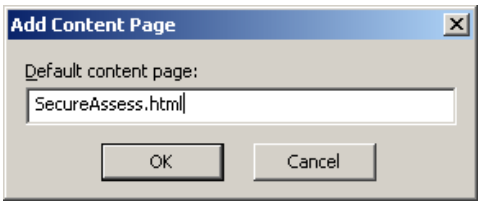
Don't exit the Properties dialogue just ye though.

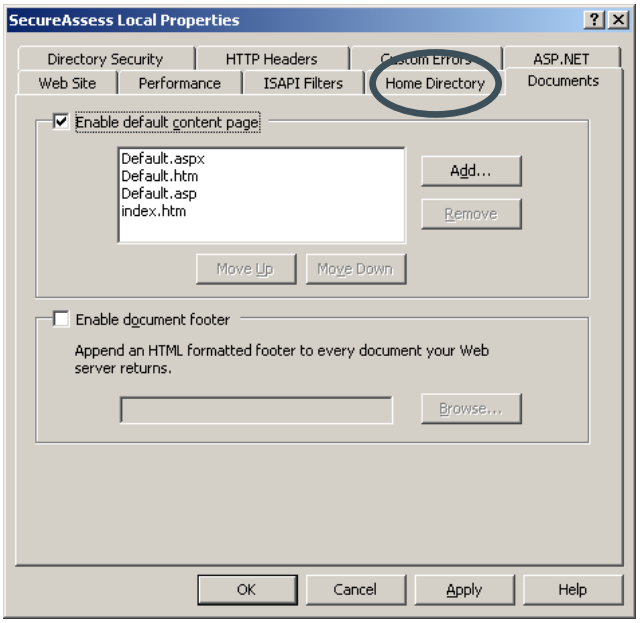
Click the Documents tab.

You should now create a new HTML page.

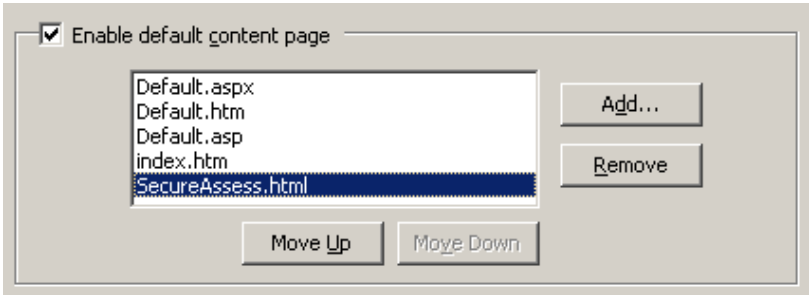
To do this:

- Click 'Add'.
- A pop-up dialogue will be displayed. Enter SecureAssess.html in the text field.

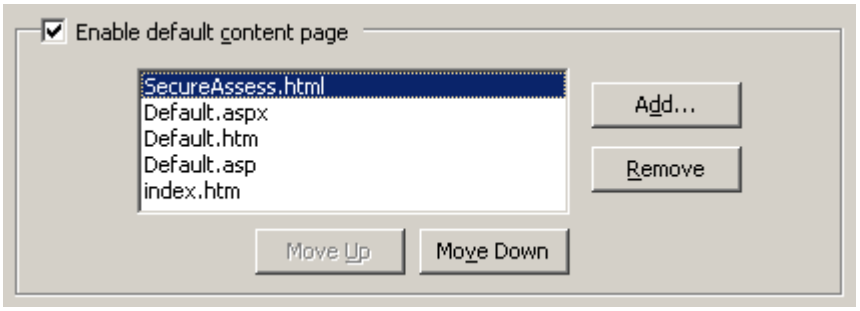




- Click 'OK'.
- The newly created page will be displayed in the content page list.
- Click the SecureAssess.html page in the list to select it, if it isn't selected already.



- Now click 'Move Up' and keep doing so until the SecureAssess.html page is at the top of the list.



- You can now click 'Apply' and then 'OK' to confirm and close the Properties window.
- Now follow the steps in Appendix 7 to complete this process.

Appendix 7: Configuring SecureAssess Local to operate on a custom port

This may be necessary when port 80 is already in use with the Default Web Site or if you have created a new Web Site.

If the Default Web Site has been reconfigured to use a custom port number, other than the Microsoft default port 80, then the steps to create a new web site and application pool are not required.

Manual Changes to Configuration files for a Custom Port Number

There are four files that you need to make changes to:

1. SecureStateService.exe.config (5 port number changes)
2. Web.Config (2 port number changes)
3. configuration_delivery.xml (1 port number change)
4. WinServiceConfig.xml (3 port number changes)
5. Deploy.bat (1 port number change)

Windows Service

Navigate to the following location, and use Notepad or a similar text editor tool to edit the file:

1. C:\Surpass\SecureAssessLocal\windowsservice\SecureStateService.exe.config

Change URL entries within this file, wherever they refer to port 80, to another port e.g. 81.

Notepad's Edit > Replace (Ctrl + H) function is very useful here, but care must be taken to manually approve each change – 'Replace All' should not be used.

```
...
<setting name="DoTasks_SyncLocalService_Sync_Local" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/Sync_Local.asmx</value>
</setting>
<setting name="RunTasks_LocalAdministratorService_LocalAdministratorService" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/localadministratorservice.asmx</value>
</setting>
<setting name="RunTasks_UpdateHelperService_UpdateHelperService" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/updatehelperservice.asmx</value>
</setting>
<setting name="DoTasks_CandidateExamStateManagementService_CandidateExamStateManagementService"
serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/CandidateExamStateManagementService.asmx</value>
</setting>
<setting name="DoTasks_MembershipService_MembershipService" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/MembershipService.asmx</value>
</setting>
...
```

Note: In the code above, the port number has been highlighted in bold and red.

When you've finished editing the config file, save it (Ctrl + S) and close it.

Next, click Start > Run and enter 'services.msc'.

Right-click on 'SecureStateService' (this will be SecureAssess Local Helper Service) and select Restart.

This will cause the service to pick up the new settings from the amended configuration from this point forward.

Web Directory

Repeat the same port editing process for the following files:

2. C:\Surpass\SecureAssessLocal\WebDirectory\Web.Config

```
...
<add key="SecureAssess_TempPDFURL" value="http://SERVERNAME:80/secureassesslocal/PDF/GeneratedPDFs/"/>
<add key="secureContentRequestUrl" value="http://SERVERNAME:80/secureassesslocal/getcontent.ashx"/>
...
```

3. C:\Surpass\SecureAssessLocal\WebDirectory\configuration\configuration_delivery.xml

```
...
<key name="secureContentRequestUrl" value="http://SERVERNAME:80/secureassesslocal/getcontent.ashx" />
...
```

4. C:\Surpass\SecureAssessLocal\WebDirectory\configfiles\WinServiceConfig.xml

```
...
<setting name="DoTasks_CandidateExamStateManagementService_CandidateExamStateManagementService"
serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/CandidateExamStateManagementService.asmx</value>
</setting>
<setting name="DoTasks_MembershipService_MembershipService" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/MembershipService.asmx</value>
</setting>
<setting name="DoTasks_SyncLocalService_Sync_Local" serializeAs="String">
        <value>http://SERVERNAME:80/secureassesslocal/Sync_Local.asmx</value>
</setting>
...
```

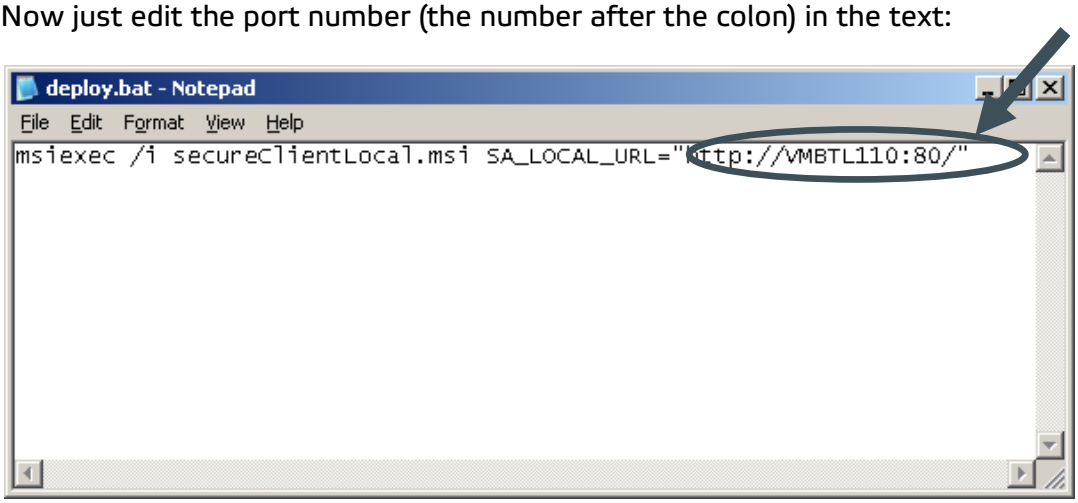
Save (Ctrl + S) each file when you've finished editing it.

5. C:\Surpass\SecureAssessLocal\WebDirectory\Installers

Right-click the “deploy.bat” file and click Edit.

This will open the .BAT file in Notepad.

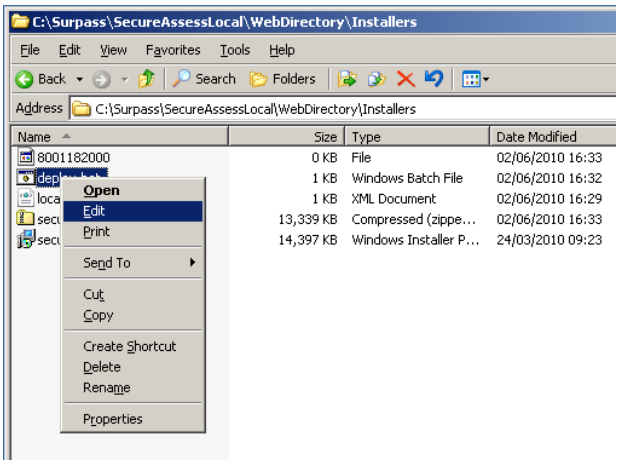
Now just edit the port number (the number after the colon) in the text:



Alter the port number and then select File > Save.

Close the Notepad.

Now, when you install the SecureClient, it will be configured to connect properly to the SecureAssess Local server.



Appendix 8: Changing the IUSR Account in IIS

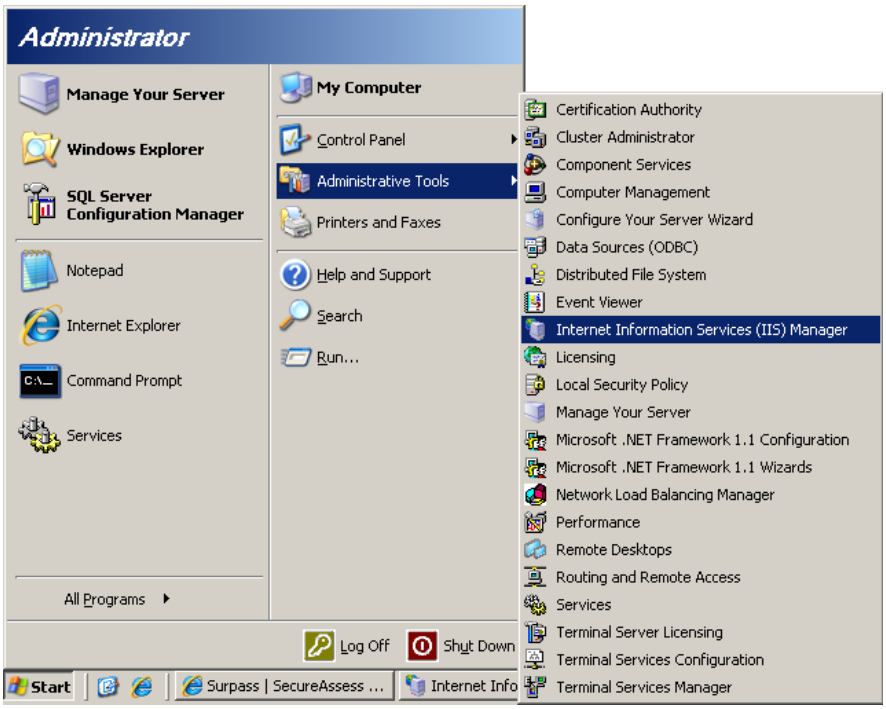
If you receive an error message when trying to enter your Keycode in the SecureClient then it may be due to the IUSR account settings in IIS.

To check and rectify this:

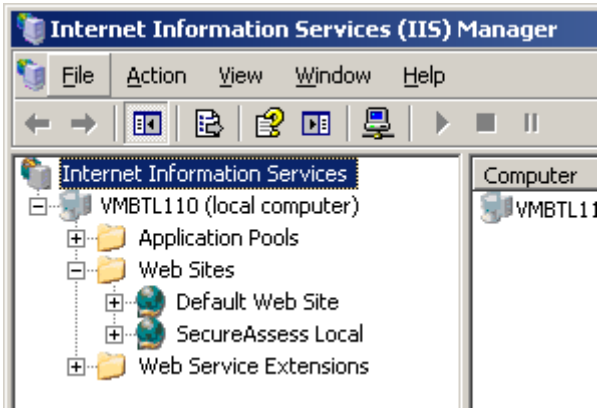
1. Open IIS Manager

   Start > Administrative Tools > Internet Information Services (IIS) Manager

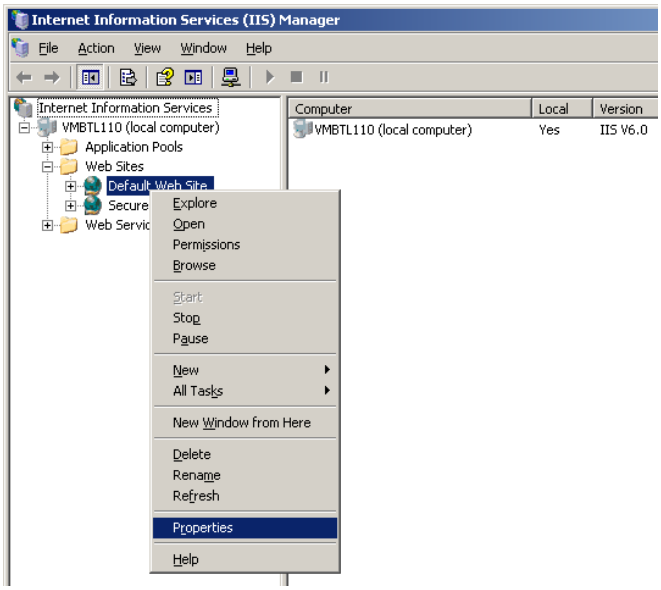
   Note: if Administrative Tools is not available from the Start Menu then you can access it by opening the Control Panel and then double-clicking the Administrative Tools icon there.



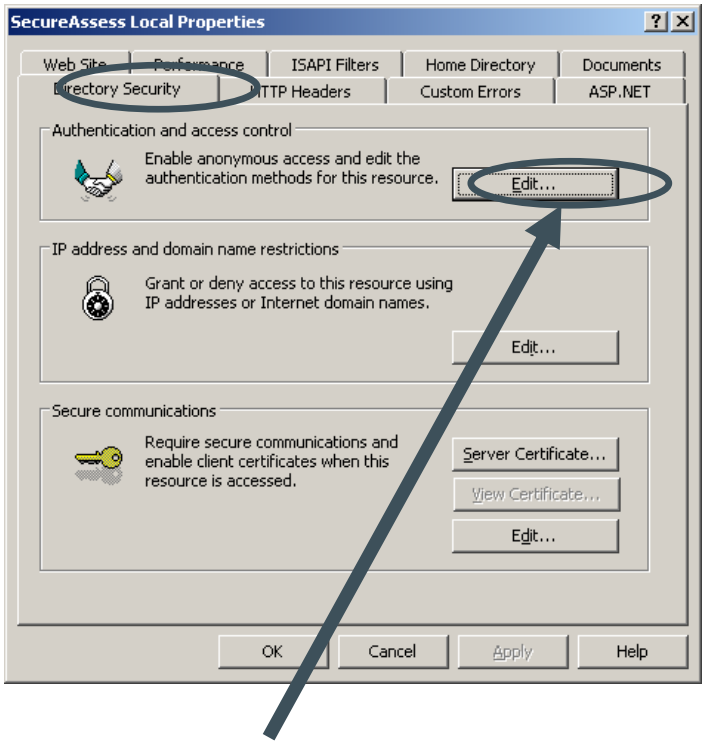
2. Expand the tree structure in the left-hand panel and then expand the Web Sites directory (by clicking the [+] symbol).



3. Right-click the Default website on the tree structure and select Properties from the displayed context menu.

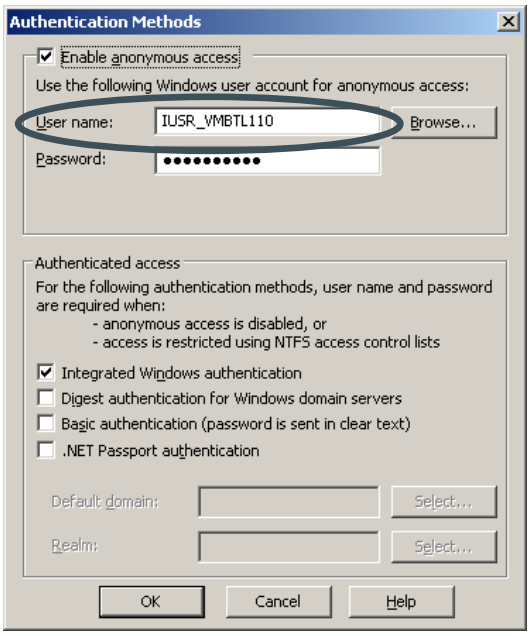


4. The Properties dialogue will be displayed. Click the Directory Security tab.



Now click the Edit button beneath the Authentication and access control heading.

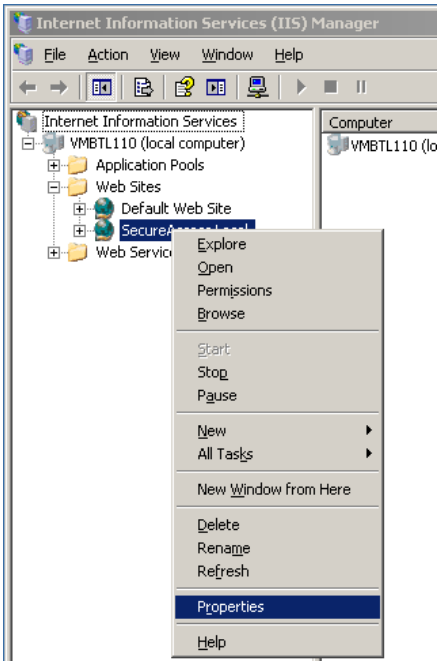
5. Examine the text in the User name field towards the top of the Authentication Methods dialogue.



Select and copy (Ctrl + C) the text in this field or write it down.

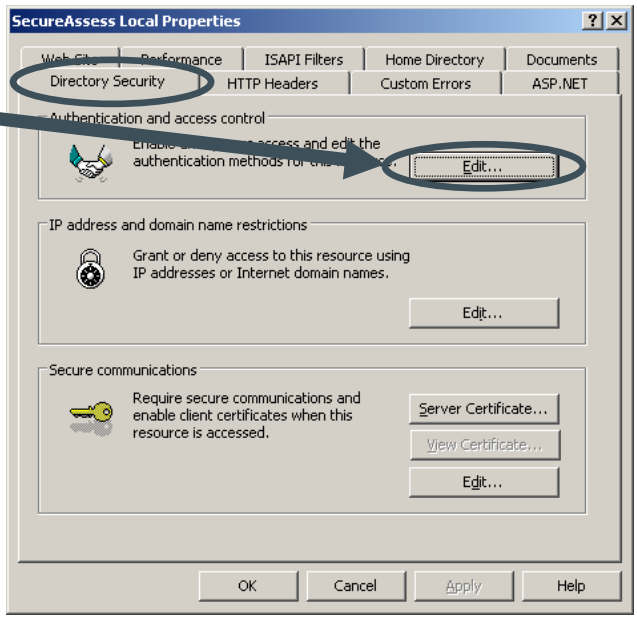
You can close the dialogue now by clicking 'Cancel'.

6. Now right-click the SecureAssess Local Website on the tree structure in the left-hand panel of the IIS Manager.

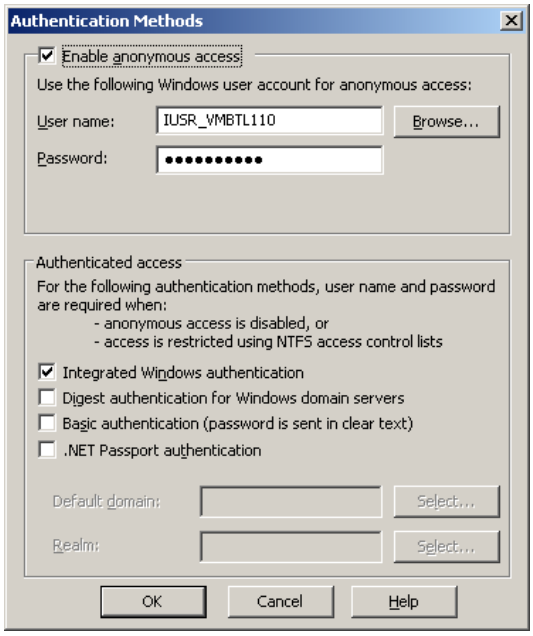


7. The Properties dialogue will be displayed and then click the Directory Security tab.

Now click the Edit button.



8. If the User name is different to the one you found for the Default website (Step 5) clear the text in the User name field and then paste (Ctrl + V) or type the information from Step 5 into the field. If the User name is the same as the one you found for the Default website then please contact the BTL Service Desk for further assistance.



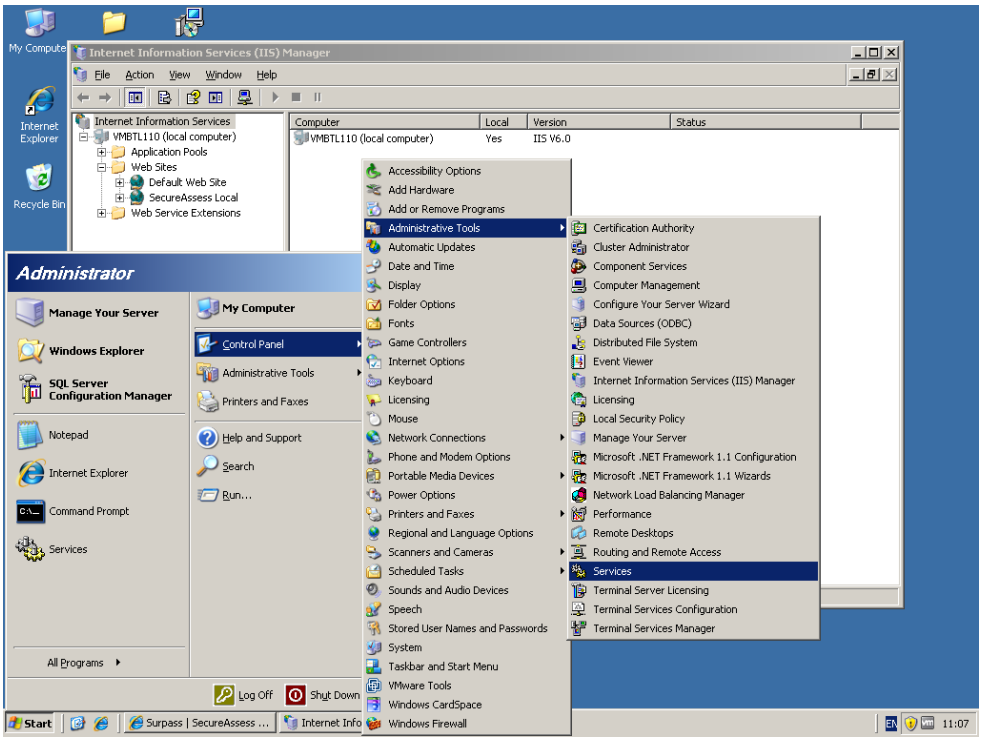
Note: You don't need to change anything in the Password field.

9. Click 'OK' to confirm the changes to the SecureAssess Local website.

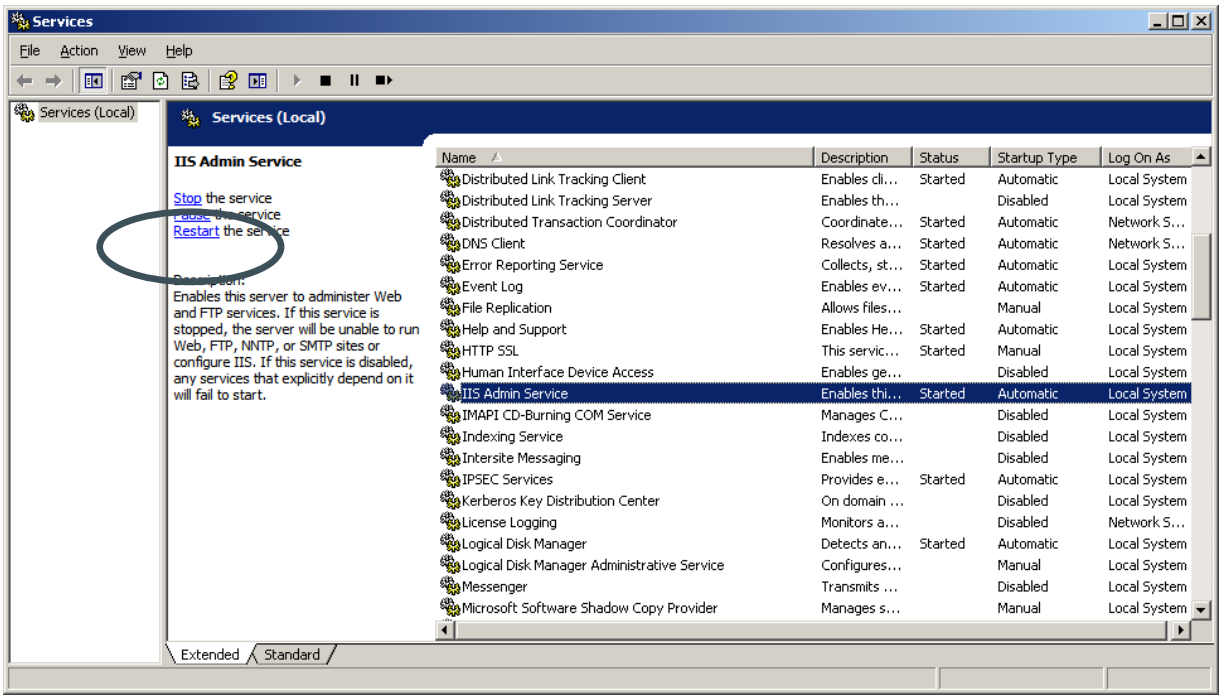
10. Now you must restart the IIS Service. Open Services by going to:

    Start > Control Panel > Administrative Tools > Services

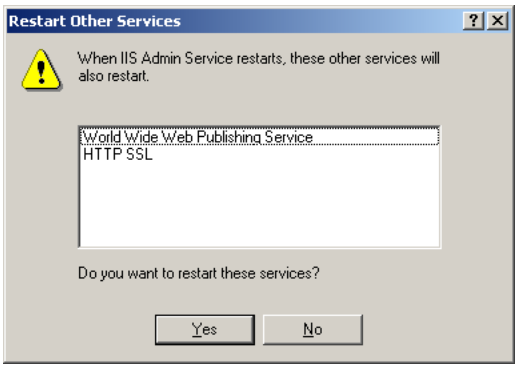
    Note: if Administrative Tools is not available from the Start Menu then you can access it by opening the Control Panel and then double-clicking the Administrative Tools icon there.



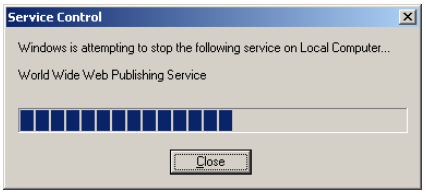
Locate the IIS Admin Service in the list, click to select it and then select Restart from the available actions on the left-hand side of the Services dialogue. Alternatively, right-click the IIS Admin Service and select Restart from the displayed context menu.



11. A pop-up may be displayed at this point, warning you that other services will also be restarted. Click 'Yes'.



12. A processing dialogue will then be shown.



13. Wait until the operation has completed. The service has now been restarted.

14. Return to the SecureClient and try to run an exam with a Keycode again.

15. If you still receive an error message when trying to access an exam using the SecureClient, please contact BTL's Service Desk for further assistance.

Document Change Record

Document Version	Description	Chapter
1.0	Removed SecureClient (Local) install instructions and test. These now form their own guide "SecureClient (Local) Install Guide and Test"	Install SecureClient and test