Access Control

FaceKey Biometric Security Suite

Software User Manual

Connecting people and information

RINGDALE

Version 4.0 April 2004

DISCLAIMER

Ringdale UK Ltd. reserves the right to revise this publication and to make changes from time to time to the contents hereof without obligation to notify any person or organisation of such revision or changes. Ringdale UK Ltd. has endeavoured to ensure that the information in this publication is correct, but will not accept liability for any error or omission.

Because of the fast pace of software development it is possible that there will be minor differences between the manual and the program.

Part No. 62-14410101

Contents

FaceKey Client Software

Introduction

The FaceKey Biometric Security Suite provides an integrated security system for access control. The Biometric Access Controller is installed inside the secure area. The camera, fingerprint or ID card reader are installed outside the secure area.

Each controller can manage the use of up to two door strikes or bolts (or one of each if required) to allow access control of up to two doors. Combinations of cameras, fingerprint readers and ID card readers are used to restrict access through the door/s using high technology 'biometric' systems that offer the very highest level of security.

The combination used will be dependent on the requirements of each installation; for example, an area requiring very high security might need the double protection of a camera for face recognition and a fingerprint reader, while in another area a fingerprint reader working with an ID card reader would be sufficient.

Ringdale's face recognition technology identifies an individual based on the unique elements of each person's face. Users initially register onto the system by posing for the USB Cam of the FaceKey Control Centre Server Software (any networked PC can be used as the FaceKey server). Each Biometric Access Controller has client software installed which then recognises the face when presented to the USB cam located at a door and grants access accordingly.

The finger recognition technology identifies an individual based on the unique elements of each person's fingerprint with no need for cards, keys, passwords or PINs (though the system can be run with an optional card reader attached to provide a double level of security if needed). Users initially register onto the system by providing one or two fingerprints to the FaceKey Control Centre Server Software - and a card ID if required .

It is important to note that the fingerprint itself is not stored anywhere, but a unique ID is created for each user based on the information taken from the fingerprint.

The client software installed on the controller will recognise the fingerprint (and card, if used) when presented at a door and grants access accordingly.

The software is used to configure the USB cam and readers to the network and provides a comprehensive level of control to allow each user to be given specific access rights. Users are assigned a security level which can be associated to selected access times for each day/date as necessary. It can also generate user and access reports as needed. The Control Centre Server software can manage multiple controllers over the network.

This manual details how to configure and use both the Control Centre Server Software and the Client Software.

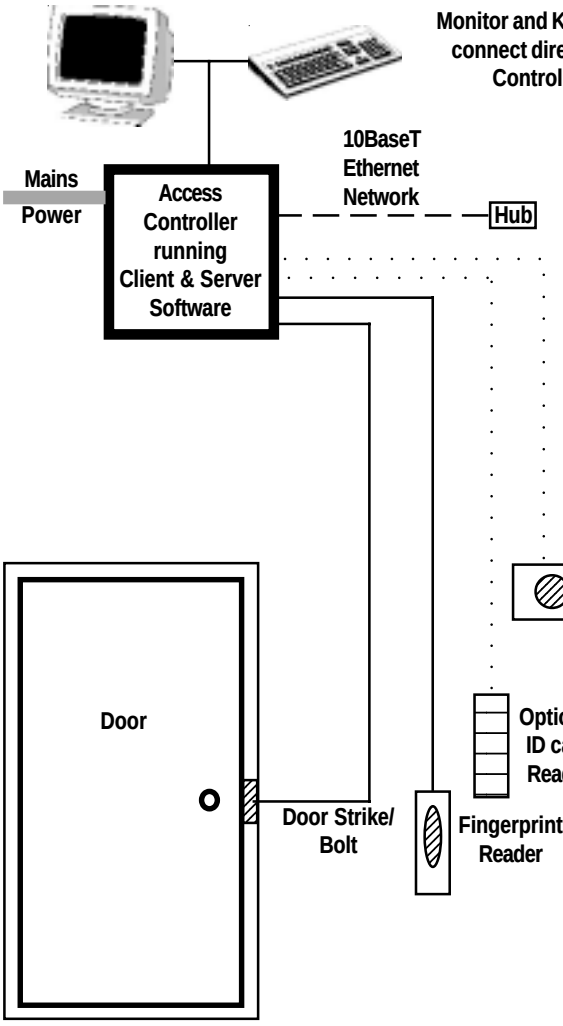
For the hardware installation please see the separate manual.

Important: The FaceKey Biometric Security Suite is shipped from the factory with both the server and client software installed on the CPU of the controller. Both programs can be operated alongside each other from here if required.

For convenience, administrators might wish to acquire a second USB cam, fingerprint reader or ID reader and install the server software on a network PC to allow user registration from their own desk.

How the Security Suite Works

Below is the set-up for the FaceKey Biometric Security Suite as supplied from the factory:

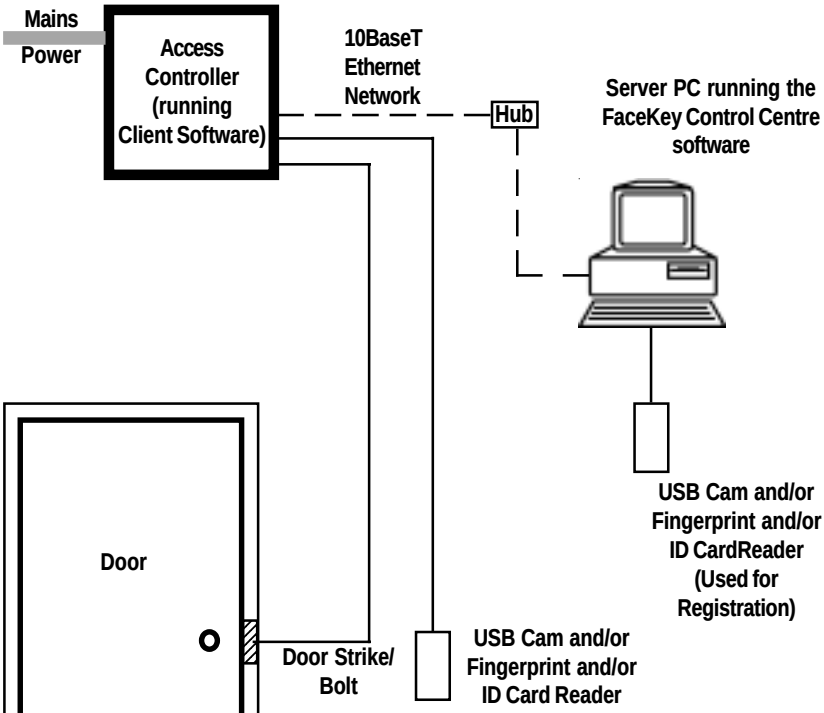


Both client and server software are installed on the controller.

User registration and access control are both performed from the controller.

Typical Set-Up Example

Below is a typical example of the set-up for the FaceKey Biometric Security Suite - with the server software installed on a remote networked PC to allow user registration and administration from the administrator's own desk:



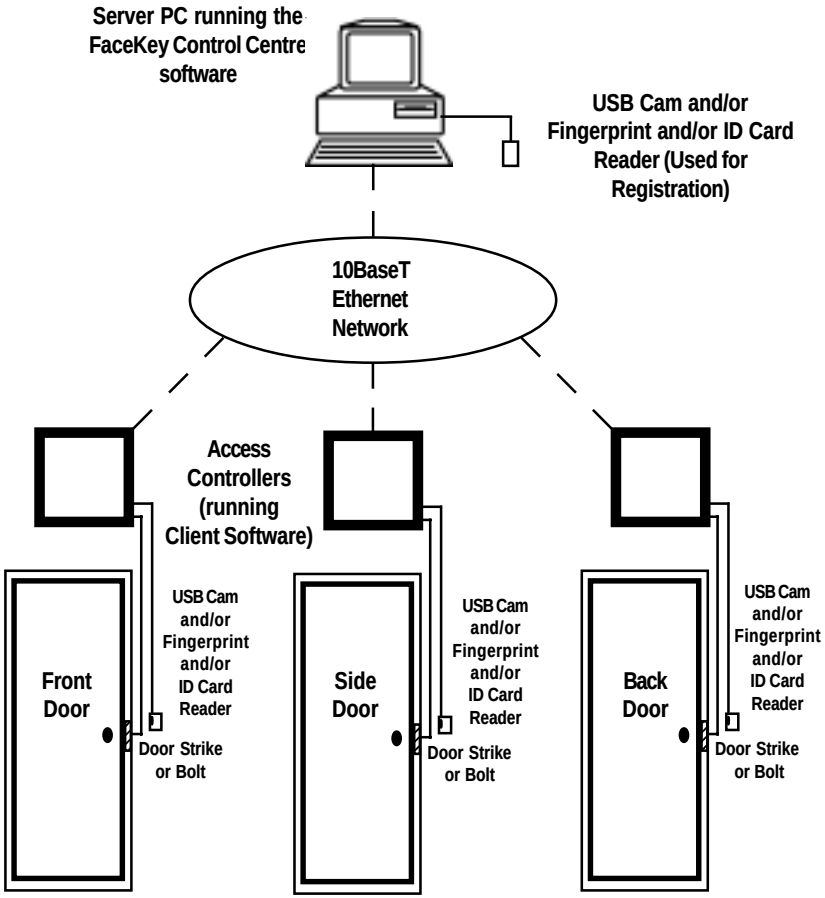
The client software is installed on the controller for access control. This will recognize and authorise the users to allow entry through the door.

Note: each controller can operate two door strike/ bolts if required.

Multiple Controller Management from One PC

With the server software installed on a networked PC, user registration and administration can be managed for all access points from one location. The client software on each access controller communicates over the network with the server.

Note: each controller can operate two door strikes or bolts if required.



FaceKey Control Centre (Server) Software

Installation

Install the FaceKey Control Centre Server Software on any networked Windows NT4/2000 or XP PC with USB Support.

Note: Both the client and server software are pre-installed on the access controller and can be run from there if required.

Important: The server software must be uninstalled from the access controller/s if a remote network PC is to be used as the server.

Close all programs on the PC before starting installation.

1 Put the supplied *FaceKey* CD into the PC's CD drive and locate the CD in *Windows Explorer*.

2 Select the **Fingerprint Reader** directory and double click on the **Setup.exe** icon. Follow the on-screen instructions to install the *u.are.u Integrator Gold* software (this is the fingerprint reader management software that will work invisibly on the PC).

3 Return to *Windows Explorer* and select the **Access Control** directory. Double click on **FaceKey_Vxxxx.msi** and follow the on-screen instructions until the *Select Features* window displays the option to select the *Typical* setup or a *Custom* setup.

Select **Custom** setup and click **Next**.

Ensure that the *FaceKey Server* option is selected and that the *Client* option is not (unless both programs are to be installed into a Biometric Access Controller, in which case both will need to be selected).

Click the **Next** button and follow the on-screen instructions to complete the installation.

4 Ensure PC is re-booted after the procedure is completed.

Before starting, ensure both the PC running the server software and the client PC inside the Access Controller are both installed on the network with fixed IP addresses.

Note: Both the client and server software are pre-installed on the access controller and can be run from there if required.

Important: If installing the server software on a network PC, the program must be uninstalled from any access controller first.

The database will be automatically created at installation. The path will be displayed in the **Database Path** field of the *System Settings* window - accessed from the *Options* menu of the main screen.

To change the location, if required, click on the **...** button alongside the field.

The name of the database will be displayed in the **Database Name** field of the same window.

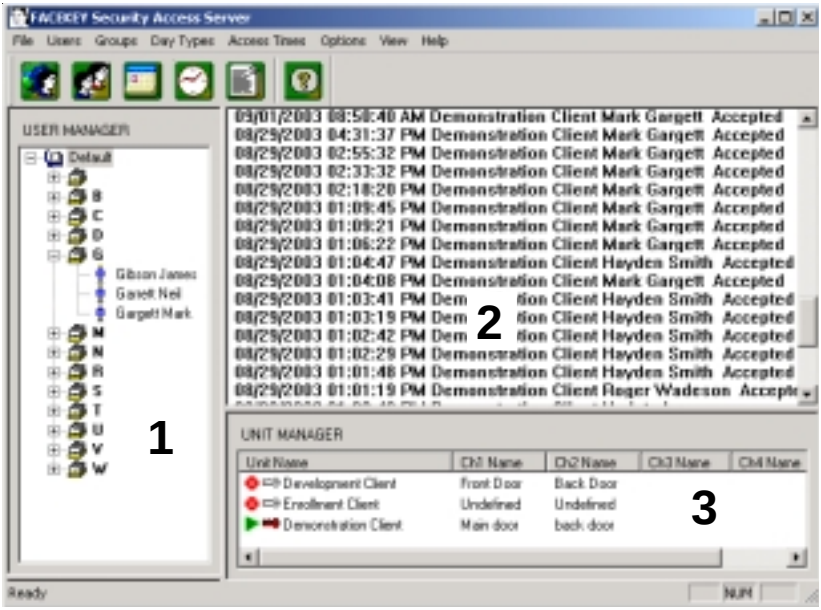
In addition, a **Log File Path** and **Temp File Path** will have been created, these paths can be altered as required by clicking on the **...** button alongside the respective field in the same window.

Also in this window, the default **Connection Port** is set to 9110, this can be changed if required. **Important: if the connection port is changed, the port setting in the *Client* software will need to be changed to match it.**

The Control Centre Software Main Screen

Before starting the software, ensure both the PC running the FKC Control Centre software and the client PC inside the Access Controller are both installed on the network with fixed IP addresses.

Open the FaceKey Control Centre software (**Start**/**Programs**/**FaceKey Control**). The Control Centre software main screen will be displayed, an example is shown below (**Note:** This is a view after the software has been configured - on viewing for the first time these fields will be blank):



IMPORTANT: Both the Control Centre and Client Software should be kept running at all times.

Following are details of the information displayed in the three fields:

Field 1
This field displays the database's list of users that have been enrolled for FaceKey.

The users entered into the database will be displayed automatically in alphabetically listed directories. To view the database navigate the branching structure in the usual *Windows* way.

Field 2
This field will display a list of events that have occurred, including:

1 Each time a user accesses a door the event will be logged and appear in field 2. Information displayed will include the name of the user, the date and time of the event, and the Access Controller used.

2 Each time an unauthorized individual attempts to access the door this event will also be displayed with the words *Unknown User*. The date, time and Access Controller involved will also be displayed.

3 If an Access Controller becomes disconnected from the Control Centre this event will be displayed in Field 2. Similarly when a controller first communicates with the Control Centre the event will be acknowledged in this field.

4 Any time updated information is sent to a remote Access Controller, the update will be acknowledged in this field.

Field 3
This field displays a list of Access Controllers (Units) that are currently associated with the control centre software. Details shown include the *Unit Name*, and the name of each *Channel* for each individual unit, as well as the current status of each unit.

Once the FaceKey client software is configured on each unit (see the second section of this manual for details on this), the unit will be automatically associated with the control centre

software and will be displayed on the list. If a unit is not displayed in this field check that the client is configured correctly.

When new data is entered into the control centre software (for instance if a new user is added) this information needs to be sent to the Access Controller (the program will ask when the change is made if the unit should be updated).

The following icons alongside each unit indicate the current communication status between the unit and the server:

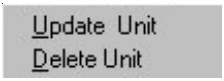
Red Crossed Circle - No communication - Client may not be running or the network might be down.

Green Arrow - Client is running and is in contact with the Control Centre.

Green Key - Unit has up-to-date data.

Red Key - Unit does ***Not*** have latest data - the unit needs to be updated (see below for details of how to do this).

Right clicking on an Access Controller on the list will display the following pop-up menu:



The **Update Unit** option provides a quick method to instantly update the selected Access Controller with the latest information from the control centre.

After this the key icon will turn green, the update will be acknowledged and an FU message will appear in the Events field (2).

The **Delete Unit** option will remove the selected unit from the list - this is for use with dead associations, for example when an existing unit has been removed from the network but its details remain in the control centre software. Deleting a currently associated unit will result in the unit immediately associating itself again and reappearing immediately.

Main Screen Toolbar

The following features can be accessed by clicking on the icons on the toolbar at the top of the screen:

Add User
Click this to add a new user. For full details on this see the chapter *Adding a New User*.

Group List
Click this to display the *Group List* window. This will show all groups and allow them to be edited/new ones to be created. For full details on this see the chapter *Adding a Group*.

Day Type List
Click this to display the *Day Type List* window. View, edit and create new day types here. For full details on this see the chapter *Adding a Day Type*.

Security Level
Click this to view/edit and create new security levels and the access times for each level. For full details on this see the chapter *Security Levels and Access Times*.

Report Options
Click this to create a user or access report. For full details on this see the chapter *Creating Reports*.

Main Screen Menu Options

The following features can be accessed from the drop-down menus at the top of the screen:

File Menu

New
Select this to create a new database (.Mdb file - it is ***Not*** necessary to have Microsoft Office installed).

Note: a default database will already be present so it is not necessary to create a new database when first starting off.

New databases will be required in environments of high usage as each database can hold up to 10,000 events - for example, with a company that is averaging 8,000 events a month, it makes sense to create a new database for each month for a logical and easy to access record.

All current users and settings (including day types, access and security levels etc.) are carried forward when a new database is created so there is very little setting up required. Just give the new database an easily identifiable name. As many databases as required can be created.

Open
Select this to open a database. A browser window will display all databases in the default directory.

Users Menu

Note: these options can also be accessed by right clicking in *Field 1* of the main screen.

Add New User
Select this option to add a new user for FaceKey.

Edit Selected User
To make changes to the details of an existing user, select the user in *Field 1* and then select this option. Make any changes as required.

Delete Selected User
To delete an existing user, select the user in *Field 1* and then select this option. All details will be removed.

Groups, **Day Types** and **Access Times**

Clicking these options provides an alternative to using the icons on the toolbar.

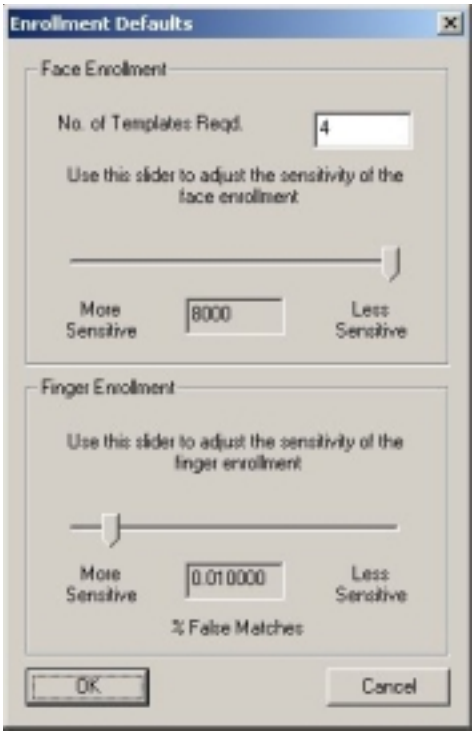
Options Menu

System Settings

This option is used when changing the configuration settings of the control centre software (for example, changing the location of the database etc.) See the previous chapter *Installation* for details on this.

Enrollment Thresholds

Selecting this option will display the following dialog box:



Use the **No. of Templates Reqd.** field to change the number of face templates created for each new user (see the face recognition section of the *Adding a New User* chapter page for details on this).

Use the slider to adjust the face enrollment threshold from more sensitive to less sensitive - because the circumstances for

each installation will be different, for example the lighting level will be variable, it might be necessary to make the software less sensitive in darker environments etc.

Important: the more sensitive the slider is set to, the less chance there is of an incorrect acceptance, but this will also make an incorrect rejection more likely. It will be necessary to find a compromise best suited to the specific environment of the installation.

Use the **Fingerprint** slider to adjust the fingerprint enrollment threshold from more sensitive to less sensitive as required.

Fingerprint reader settings are a trade-off between accuracy and useability. The higher the level of accuracy that is set as a requirement, the greater the difficulty there will be in achieving an acceptable reading. By default, the fingerprint reader is set with a false accept threshold of one in ten thousand (the likelihood of an unauthorised fingerprint gaining access).

In certain situations a higher threshold will be required (for example in installations where security is very important). In this scenario the accuracy required for acceptance will be greater, therefore there will be an increased rejection rate for fingers that are not placed cleanly on the reader. The fingerprint reader can be set to a false accept threshold of up to one in one hundred thousand.

In other situations where there is a high level of usage but security is not of paramount importance (the fewer rejections the better) it might be preferable to lower the false accept threshold. The fingerprint reader can be set to a false accept threshold as low as one in one thousand.

Click **OK** to save any changes made.

Rotate Image
This option allows the image presented by the Enrollment camera to be rotated if required - for example if the position best suited to the camera is on its side, then this facility would be required to ensure the image was presented the correct way up.

Change Password
When accessing user's details a password is required for security purposes.

The default password is **password** (all lower case).

Use this option to change the password as required.

Important

The same password that is used for the control centre software will need to be used for the client software so that the two applications can communicate with each other.

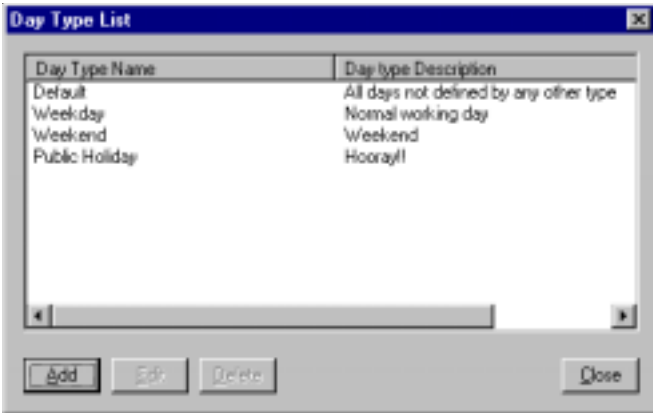
Adding a Day Type

The FaceKey control centre provides a sophisticated access and security setup to allow a high level of management for all users. The first part of this is setting up different day types which can then be assigned different access hours for different security levels. When a user is added the security level required for that user can then be selected (these later procedures are dealt with in the next chapter). This chapter is concerned only with setting up day types.

Note: if all users can have full access 24 hours a day, seven days a week, 365 days a year, then this feature does not need to be configured, move straight on to the next chapter *Security Levels and Access Times*.

Following is a simple example to demonstrate how a day type model can be created:

1 Click on the **Day Type List** icon on the toolbar (shown here) to display the following window:



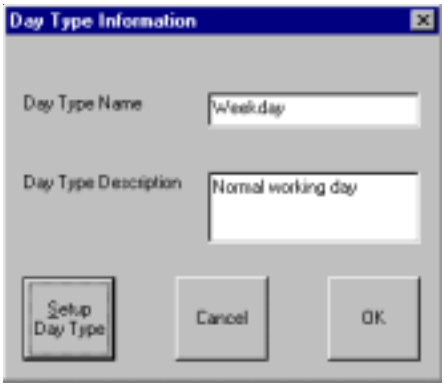
Note: This example shows the day type model already created. The first time this window is opened there will be only one entry on the list, which will be **Default**.

The day type list created here is very straightforward. All days are accommodated into three categories.

Weekdays
Weekends
Public Holidays

As all days in the calendar are covered by these three categories the *Default* option on this list would not be used, but the list offers a great deal of flexibility (for example, the default category could be used as the weekday category). As many day types as required can be created, so the list can be built to suit any number of needs.

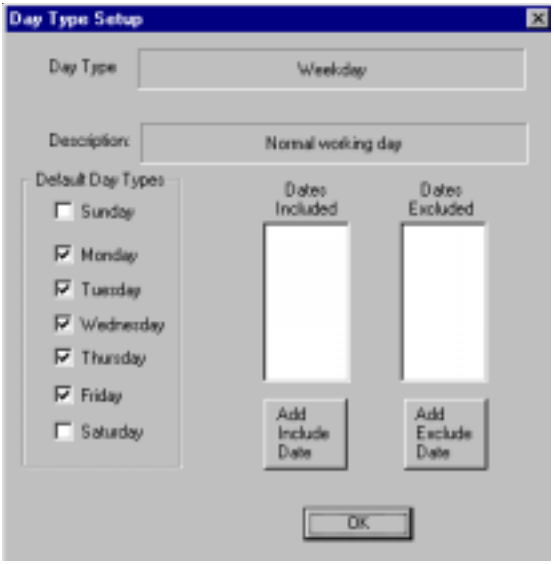
2 Click the **Add** button to create a day type. The following window will be displayed:



Enter a **Day Type Name** and a **Day Type Description**.

3 Click the **Setup Day Type** button to display the window shown following. Because this example is for a weekday day type, all the tickboxes for weekdays need to be checked. If creating another day type specific to a certain scenario, check whatever days are required.

Use the **Add Include Date** button to add a specific date to be included in the day type. When clicked a calendar will be displayed. Scroll the calendar to select the date required and click on the number to select it. The date will appear in the *Dates Included* field.



Use the **Add Exclude Date** button to add a specific date to be excluded from the day type. When clicked a calendar will be displayed. Scroll the calendar to select the date required and click on the number to select it. The date will appear in the *Dates Excluded* field.

4 Click **OK** to save the settings and then click **OK** again to save the day type. The day type will appear in the list of the *Day Type List* window.

Repeat to create as many day types as required.

Important

When exiting the *Day Type List* window, the program will acknowledge the new data that has been entered and the key icon (displayed on the main page) for each unit will change. All the units will need to be updated for the changes to take effect.

Once the day types have been added proceed to the following chapter *Security Levels and Access Times* to complete the access control configuration.

Changing Day Type Details

The details set up for each day type can be changed at any time by selecting the day type from the list and clicking the **Edit** button.

Deleting a Day Type

A day type can be removed from the list at any time by selecting it and clicking the **Delete** button.

Important: ***ensure that the day type has been disassociated from all security levels before removing it - user's access rights could be affected.***

Security Levels and Access Times

The FaceKey control centre provides the ability to create different security levels that can be granted different access times, giving a high level of flexibility and control for an infinite variety of scenarios.

Note: if all users can have full access 24 hours a day, seven days a week, then only very basic configuration is required. Use the default security level and set the access time to 24 hours.

Following is a simple example to demonstrate how the system works:

Company A uses three security levels

Supervisor - for managers and directors

General Staff - for all other staff

Cleaner - for out of hours cleaning staff

They use the *Default* security level as a kind of 'pending' area as they have chosen to have no access granted for this level. New members of staff could be assigned to this level while awaiting confirmation of their actual security level - *Default* doesn't have to be used this way, it can be set with any access times the same as any other level (though it should not be renamed or its description altered).

If no security level is assigned to a user when they are added they will automatically be assigned to the *Default* level.

The company uses three day types (as previously described):

Weekdays

Weekends

Public Holidays

On weekdays, employees assigned to the *General Staff* security level can only gain access between the hours of 8.00 am and 7.00 pm.

On weekends they are not allowed access at all.

On public holidays they are allowed access only between 10.00 am and 4.00 pm

Managers/directors assigned to the *Supervisor* security level have unlimited access on weekdays, weekends and public holidays.

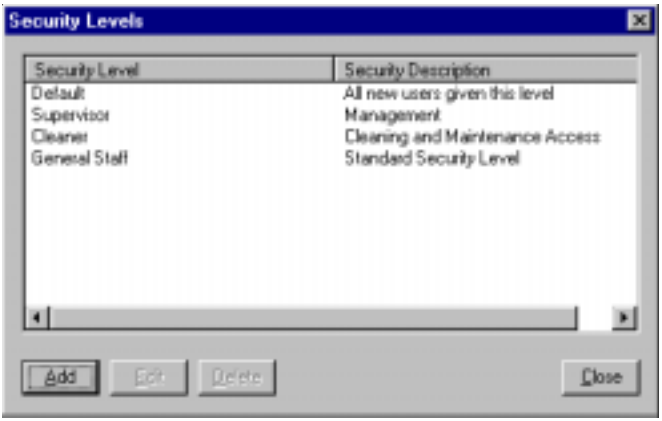
Cleaning staff - assigned to the *Cleaner* security level - are not allowed access on weekends or public holidays

On weekdays they are granted access between the hours of 6.00 am and 8.00 am, and 6.00 pm and 8.00 pm.

Creating a Security Level

Use the following procedure to create a security level:

1 Click on the **Security Level** icon on the toolbar (shown here) to display the following window:



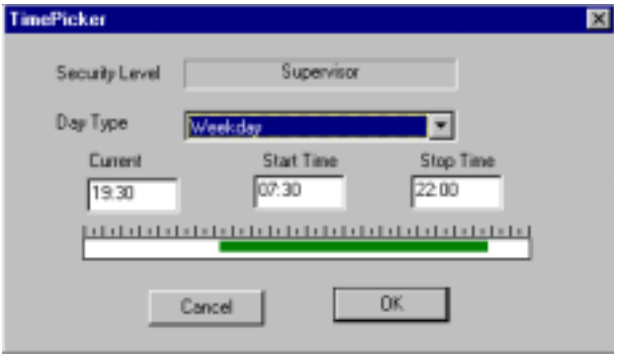
Note: This example shows the security level model already created. The first time this window is opened there will be only one entry on the list, which will be **Default**.

2 Click the **Add** button to create a security level. The following window will be displayed:

Enter a **Security Level Name** and a **Security Level Description**.

Setting Up Access Times for the Security Level

3 Click the **Setup Access Times** button to display the following window:



From the **Day Type** drop-down box select the day type the access time will be assigned to (the day types were created in the previous chapter).

Then use the *TimePicker* to select the access time required. Move the cursor across the time bar and the time will be

displayed in the *Current* field above it. Hold the left mouse click down at the start time and drag up to the end time. Release the mouse click at the end time.

A bar marking out the access time will appear. Move the cursor out and then back in to the timebar to update the *Start* and *Stop* times in the fields above the bar.

To save multiple time zones in the same day type, hold the control key down and repeat the above procedure to create as many zones as required.

Important

To save the time zone that has been created click the **OK** button after every day type has been set. To set up another day type re-open the timepicker window and repeat the procedure.

4 Click **OK** to return to the *Security Levels* window. The new security level will be displayed on the list. Repeat to create as many security levels as required.

Important

When exiting the *Security Level* window, the program will acknowledge the new data that has been entered and the key icon (displayed on the main page) for each unit will change. All the units will need to be updated for the changes to take effect.

Changing Security Level and Access Time Details

The details of each security level can be changed at any time. Select the security level required from the list in the *Security Levels* window and click the **Edit** button. The windows previously displayed can be accessed and changed as required.

Deleting a Security Level

Select the security level required from the list in the *Security Levels* window and click the **Delete** button.

Important: ***if a security level is to be deleted, ensure that all users assigned to that level have been moved to another first. Any users left could lose their access rights.***

Setup for Basic Configuration

It might be that the advanced access control features discussed in this chapter are not required. If all users can have full access 24 hours a day, 365 days a year, the setup procedure is very straightforward.

Select the **Default** security level from the list in the *Security Levels* window and click the **Edit** button.

Click the **Setup Access Times** button and ensure that the **Default** day type is selected from the drop-down box - no day types need to be created.

Drag the cursor fully along the time bar so that the full 24 hour period is selected. Click **OK** twice and close the *Security Levels* window.

FaceKey is now configured to give all users full access at all times.

Adding a New User

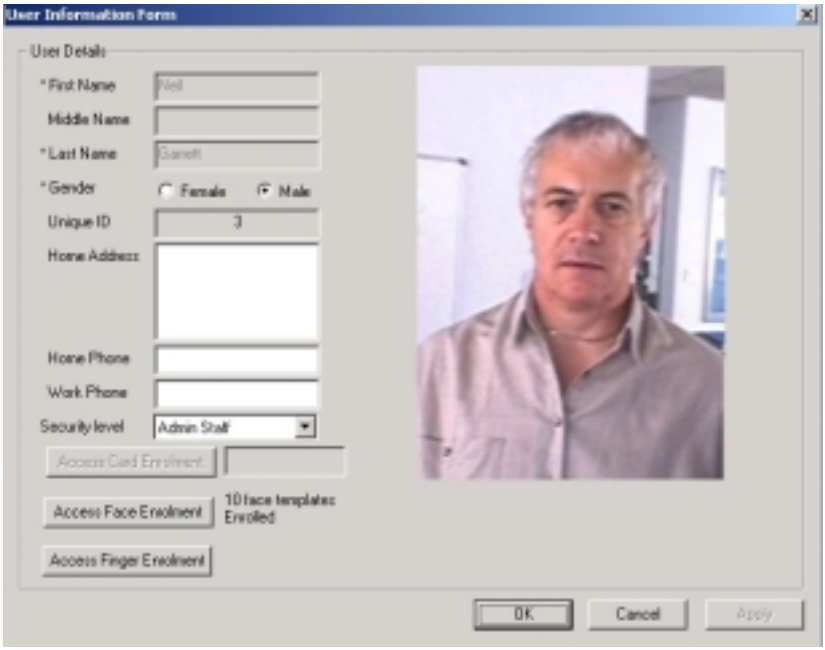
Click on the **Add User** icon on the toolbar (shown here) to display the *New User* window shown below (**Note:** this example shows a typical setup with the new user's details added. When this window opens all fields will be empty.)

Important

Whenever the *New User* window is selected, entry of a password will be required to gain access. The default password is set to:

password (all lower case)

Because of the sensitive information accessed here it is highly recommended that a password be set straight away. Select **Change Password** from the *Options* menu on the main screen to do this.



Enter the information for the user. The **First Name**, **Last Name** and **Gender** fields ***Must*** be filled in. Other fields are optional.

From the **Security Level** drop-down box select the security level the user is to be assigned to (see the chapter *Security Levels and Access Times* for full details of this feature). If a security level is not selected here a user will automatically be assigned to the *Default* level. If the security levels feature is not to be used just leave each user in the *Default* level.

The next steps will be dependent on which access control options are being used - select up to two from the following.

1 Face Registration

2 Finger Registration

3 ID Card Registration

After the registration is complete for the user, the **Unique ID** field will display the number that the control centre has assigned to that user only.

Face Recognition

Important

The Control Centre software creates several face templates when registering each new user, and uses all of these templates when searching to identify a face that is presented to the camera. This helps to provide fast and accurate identification. This means that during the registration the face will need to be presented several times. By default, this is set to five. This can be changed if required - select *Enrollment Thresholds* from the *Options* menu of the main screen to do this.

It is advised that the registration of new users takes place in a well lit area.

To register a user for face recognition use the following procedure:

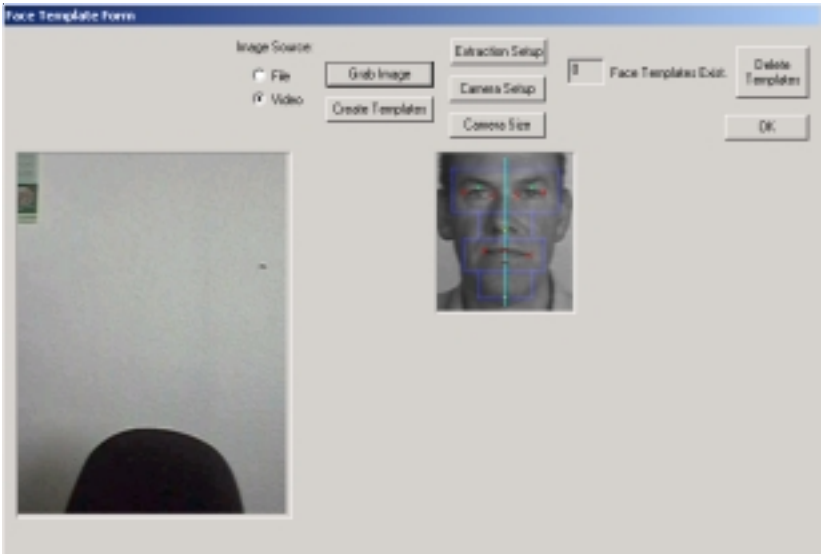
1 Click on the **Access Face Enrollment** button to display the window shown following.

2 The registration can be made in one of two ways:

(i) using an existing photograph by selecting the **File** option under *Image Source*. Browse to the location of the file and click OK to display the image in the bottom left side of the window.

(ii) Taking the image direct from the camera feed in real time (with the user presenting themselves to the camera). Select the **Video** option under *Image Source*. The feed from the camera will be displayed on the screen.

Click on the **Grab Image** button to save a reference image to the database. This will be displayed in the previous *New User/Edit User* window along with the user's other details.



Creating the Face Templates

To start creating the templates click the **Create Templates** button. If the direct feed from the camera method is being

used, captures will be made of the image which will then be displayed on the right side of the window. The software will then attempt to create the template from the image. If it is successful a dialog box will appear confirming this. Click **OK** and the software will move on to the next template until all have been completed. If the software is unsuccessful it will automatically capture another image and try again.

The image on the right will display coloured dots and lines which will try to be matched to the key features of the face - eyes, mouth, chin etc. With practice, it will be seen what the software is looking for in its matching, and the best position for the subject to pose in will become apparent. Try to get the face to fill the image but remain completely viewable.

Several buttons provide access to the camera configuration settings, these can be used to find the optimum set up for each individual circumstances (the options will vary according to the type of camera being used).

Important: It is recommended to keep the camera resolution at 320 x 240.

3 When the required number of templates has been created, the registration will be complete.

Have the user present their face to the client camera and use the *Debug* window in the client software (see the second section of the manual for details of this) to ensure that the user is identified.

Enrollment Thresholds

The enrollment threshold can be altered from the *Options* menu. Use the slider to adjust the enrollment threshold from more sensitive to less sensitive - because the circumstances for each installation will be different, for example the lighting level will be variable, it might be necessary to make the software less sensitive in darker environments etc.

Important: the more sensitive the slider is set to, the less chance there is of an incorrect acceptance, but this will also make an incorrect rejection more likely. It will be necessary to find a compromise best suited to the specific environment of the installation.

Fingerprint Recognition

Important Information

When registering a fingerprint please bear the following in mind:

a) Care needs to be taken when setting up users for the fingerprint reader. The more meticulous the approach taken with this procedure the clearer and sharper the image will be. The stronger the quality of data that is stored the more reliable and consistent will be the access capability of the user (the actual fingerprint is not stored, only points of reference from it). Below are some tips to help achieve this:

i Ensure the fingerprint sensor is clean (use a soft, dry cloth) before starting and that it is regularly wiped (especially if users have particularly oily hands).

ii Users should wash and dry their hands prior to the start of the procedure.

iii The fingerprint should cover as much of the sensor as possible. Place finger directly on the sensor without sliding across the surface. Repeat the action until the administrator believes optimal finger placement has been achieved.

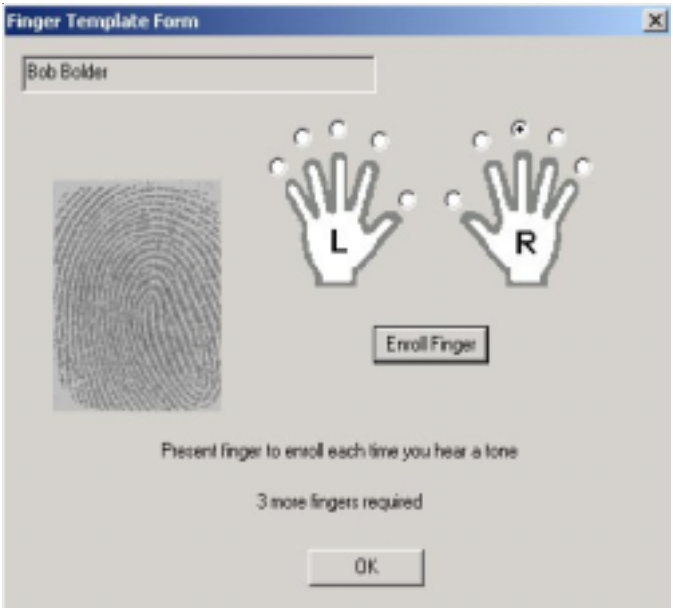
b) It is recommended that each individual registers two or three fingers. There will then be a backup print that can be used in the event of one of the fingerprints becomes temporarily or permanently altered (for example by a paper cut or minor burn).

c) Every finger registered will need to be processed four times, then verified, to ensure a thorough identification is possible.

To register a user for fingerprint recognition use the following procedure:

1 Click on the **Access Fingers Enrollment** button to display the window shown following.

2 Select the finger that is to be registered by clicking on the *Radio Button* above the fingertip.



3 Click on the **Enroll Finger** button.

Note: It is necessary to enter the fingerprint four times (+ once more for verification) for each finger that is to be sampled - this allows the software to attain a high level of recognition.

4 Register the selected finger by firmly and slowly pressing the finger tip onto the fingerprint reader connected to the Control Centre Server PC. After each press wait for the appearance of the fingerprint in the image box in the left of the window. Check the fingerprint sample counter which will countdown with each sample.

5 Present the selected finger onto the reader four times. A message will confirm that the finger has been successfully registered.

6 Present the finger to the reader a fifth time to verify that the finger can be identified.

If at any time a fingerprint is not clear a ***Not Recognized*** message will be displayed. Present the finger to the reader again.

7 Click the **OK** button to return to the *Add User* window.

If you wish to register another finger, repeat the above procedure.

Note: when returning to the fingerprint template form, fingers for that user that have already been registered will have a green light on the fingertip.

ID Card Registration

If an ID card reader is to be used and the user is to be assigned a card as part of their access rights, follow these steps to automatically load the number of the card. Note: The actual card will be needed to present to the reader.

1 Click on the **Access ID Card Enrollment** button.

2 Once this button is activated, present the user's ID card to the card reader (**Note:** the card will need to be coded with a pre-assigned number). The card must be presented within 30 seconds of the button being activated.

3 When the card has been read, the number of the card will be displayed on the screen. Click **OK** to return to the *Add New User* window. In the field next to the card enrollment button, the number of the card will be displayed.

When all the information that is required for the new user is completed, click the **OK** button.

The Control Centre main screen will now be updated with the new information. The new user will be listed alphabetically in the column on the left.

Repeat the procedure for as many users as required.

Important

Remember that when all the new users have been added, it will be necessary to update all the client units with the new information (see *The Control Centre Software Main Screen* chapter for details of this).

Viewing and Editing User Details

The details entered for each user can be viewed and amended at any time by highlighting the name in the column on the left of the main screen and selecting the **Edit Selected User** option from the *Users* menu. View/change the information as required.

If it becomes necessary to re-register a face at any time - for instance, if someone grows a beard - the face enrollment window has a **Delete Templates** button that will remove the existing templates and allow the face to be registered again.

Important

Whenever *Edit Selected User* is selected, entry of a password will be required to gain access. The default password is set to:

password (all lower case)

Whatever password is set, the password on the client software must be set to the same in order for the two applications to communicate with each other.

Deleting a User From the System

To remove a user from the system highlight the name to be deleted in the column on the left of the main screen and select the **Delete Selected User** option from the *Users* menu. The user will be removed.

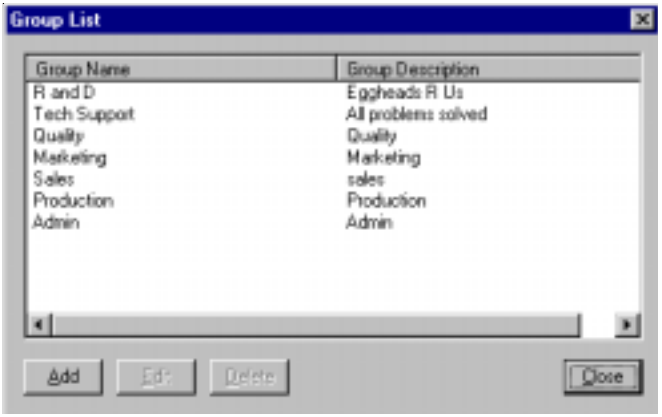
Adding a Group

The *Groups* feature is designed to help manage the users more effectively and help in the creation of reports. It is recommended that the required groups be created before the users are added, then the users can be assigned to the correct group as they are registered.

A simple way to use the *Groups* feature is to create a group for each department within the company and assign each user to the group that matches their department. When a report is generated it will then be possible to create department specific records.

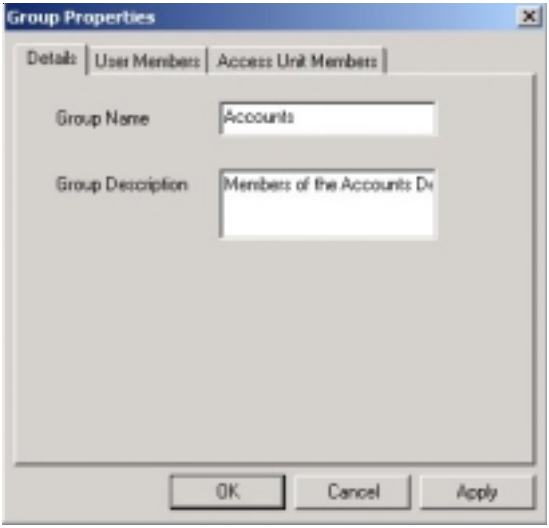
Similarly, any users who are to feature together in a report can be placed in the same group to facilitate this.

Access the *Group List* by clicking on the icon shown here (found on the toolbar on the main page of the Server Centre software). The following window will be displayed:



Note: this example shows a list once it has been set up. The first time this window is opened it will be empty.

Click on the **Add** button to create a group. Enter the **Name** and a **Description** for the group and click **OK**. The group will appear on the list.



To edit the details of an existing group, select it from the list and click the **Edit** button.

To remove a group from the list, select it and click the **Delete** button. **Important:** all users assigned to that group will be moved to the *Default* group - remember to assign them to another group if required.

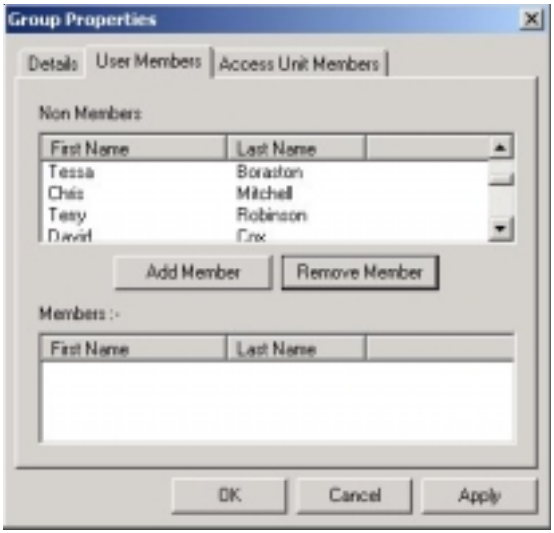
Important

When exiting the *Group List* window, the program will acknowledge the new data that has been entered and the key icon (displayed on the main page) for each unit will change. All the units will need to be updated for the changes to take effect.

Adding a Member to a Group

Note: a member can only be added to one group. If a member who has already been assigned to a group is selected for another group, they will be ***Moved*** from the old group to the new one.

Select the **Members** tab in the above window to display the page shown following (ensuring that the group required is selected first).



A list of all users will be displayed in the upper field and a list of all users assigned to this particular group will be displayed in the lower field.

Select the user to be added from the upper field, the **Add Member** button will become active. Click the button and the user will be added to the list in the lower field - and assigned to this group.

To remove a user from the group, select the user from the lower field, the **Remove Member** button will become active. Click the button and the user will be returned to the list in the upper field.

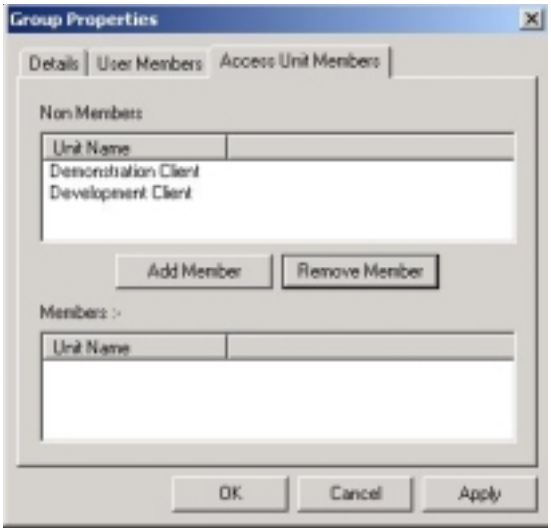
Click the **Apply** or **OK** buttons to save the changes that have been made.

Adding a Controller (Unit) to a Group

Note: an access controller can be assigned to as many groups as required.

Associate an access controller to a group using the following procedure:

Select the **Access Unit Members** tab in the *Group Properties* window of the required group. This will display the following page:



A list of all controllers not assigned to this group will be displayed in the upper field and a list of all controllers that are assigned to this particular group will be displayed in the lower field.

Select the controller to be added from the upper field, the **Add Member** button will become active. Click the button and the controller will be added to the list in the lower field - and assigned to this group.

To remove a controller from the group, select the unit from the lower field, the **Remove Member** button will become active.

Click the button and the user will be returned to the list in the upper field.

Click the **Apply** or **OK** buttons to save the changes that have been made.

Creating Reports

Access control data that is stored on the system can be used to generate reports if required. There are two types of basic report that can be created:

User Report: this will create a full list of all users that are set up on the system, listed within the groups that they are assigned to.

Details displayed about each user will include their security level, user ID number and card ID number if they have one.

Access Report: this will generate a record of access events logged by the system. A range of available options allow the record to be tailored to specific requirements - the access record of a particular user could be generated, or a group, a unit or a combination of these (for example the record of a certain user accessing through a specified unit only). The date range can also be selected as required.

Details displayed will include the date and time access was attempted, the unit involved and whether the attempt was accepted or refused.

All reports generated can be printed out if required.

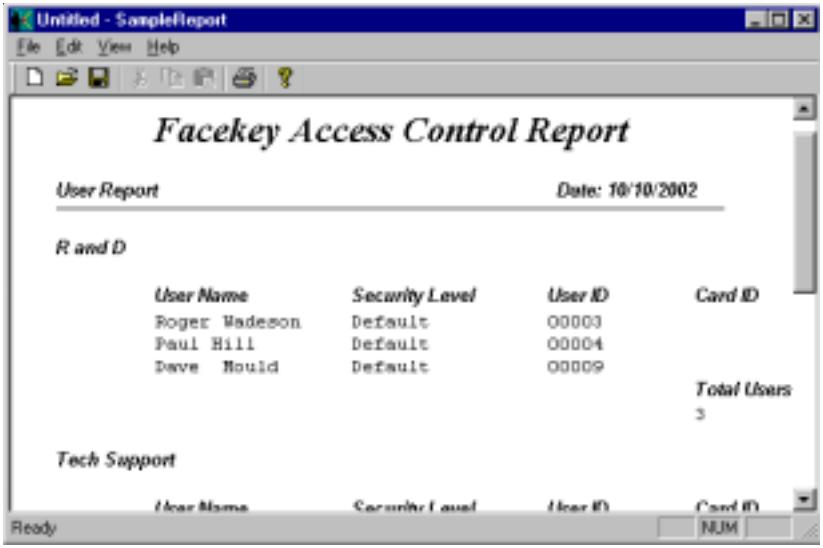
Use the following procedures to create a report:

1 Click on the **Report Options** icon on the toolbar (shown here). A browser dialog box will open on the default directory where the .mdb database files are normally stored (C:/Program Files/FaceKey/FaceKey Access Control).

Select the database required from the list, or browse to the directory where the file is stored (if the files are stored in a different directory).

Click the **Open** button to display the *Report Options* window - an example of which is shown following:

To create a **User Report** - as described previously - select this option at the top of the window and click the **OK** button. Below is an example of a user report:



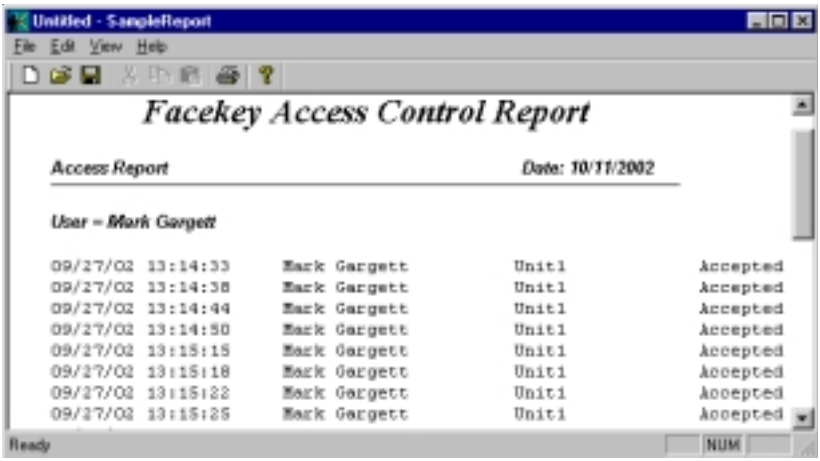
To create an **Access Report** - as described previously - select this option at the top of the window. The *Report Criteria* field will become active.

Use the tick boxes to activate the criteria required for the report and enter the **User Name**, **Group Name** or **Unit Name** as necessary (any combination of these can be used).

If all entries related to this criteria that are in the database are to be included in the report, the date features do not need to be used. But the **Start Date** and **Stop Date** options can be used to refine the search. Clicking the drop-down feature in both options will display a calendar and allow a date to be selected. Use the arrow buttons at the top of the calendar to scroll to the required month, click on the day required to select that day.

Using just the *Start Date* option will find all information in the database from that day onward. Using just the *Stop Date* option will find all information up to that date in the database. Use both options for a more refined search.

When the criteria is set as required click the **OK** button and the report will be generated. Below is an example of an access report:



This is a simple example using the criterion of *User Name* only to display all access events for the named user that are stored in the database.

Uninstalling the Control Centre Software

Important: If the Control Centre server software is to be installed on a remote network PC, the software must be uninstalled from all access controllers first.

Uninstall the Control Centre software as follows:

1 Ensure the Control Centre program is closed.

2 From the **Start** menu select **Settings/Control Panel/Add/ Remove Programs** and select **Access Control** from the list. Click on the **Add/Remove** button and the program will be removed from your PC (If the *Control Centre* and *Client* programs are installed on the same PC this will uninstall both).

Note: before attempting to install a new version of the software it is advisable to reboot the PC.

FaceKey Client Software

(Installed into the Biometric Access Controller box)

Installation

The FaceKey client software will be pre-installed onto the hard drive of the Biometric Access Controller. These installation instructions will only be required if it becomes necessary to re-install the client at some time.

Close all programs on the PC before starting installation.

1 Put the supplied *FaceKey* CD into the PC's CD drive and locate the CD in *Windows Explorer*.

2 Select the **Fingerprint Reader** directory and double click on the **Setup.exe** icon. Follow the on-screen instructions to install the *u.are.u Integrator Gold* software (this is the fingerprint reader management software that will work invisibly on the PC).

3 **Windows 2000 or XP**
Ensure that the Windows Autologon feature is activated (this enables the Client to restart automatically if the CPU is rebooted).

Windows NT4
Return to *Windows Explorer* and select the **Utilities** directory. Select the **Autolog** directory and double click on the **Setup.exe** icon. Follow the on-screen instructions to install the *Autologon* software (this enables the Client to restart automatically if the CPU is rebooted).

4 Return to *Windows Explorer* and select the **Access Control** directory on the CD. Double click on **FaceKey_Vxxxx.msi** and follow the on-screen instructions until the *Select Features* window displays the option to select the *Typical* setup or a *Custom* setup.

Select **Custom** setup and click **Next**. Ensure that the *FaceKey Client* option is selected. Click the **Next** button and follow the on-screen instructions to complete the installation.

5 Ensure the PC is re-booted after all the procedures are completed.

Configuration Procedures

Important Notes

Each biometric access controller can operate two channels. A door strike or bolt can be operated for each channel as required. If only one door strike or bolt is connected it will automatically default to channel 1.

Each channel can operate a fingerprint reader and an ID card reader. Only one channel can operate a camera (either 1 or 2 as required. The client software will automatically detect how many devices are connected to the controller.

Generally, the devices will conform to the order in which the hardware has been plugged into the access controller (see the separate hardware manual for details of installation). For example, a fingerprint reader plugged into the controller's first USB port will appear in channel 1, a second fingerprint reader plugged into the second USB port will appear in channel 2. It might be necessary to switch around the USB ports to ensure that the correct reader is in the correct channel for your requirements.

Before starting, ensure both the client PC (the access controller) and the FKC Control Centre PC are both installed on the network with fixed IP addresses.

The client software operates as a service. The service will start automatically when the PC is booted up.

The Client should be kept running at all times.

The icon shown below will be displayed in the bottom right corner of the screen (near the clock). Right clicking on this icon accesses the client software menu as shown following:

The following configuration procedures need to be completed before using the FaceKey system:

Configuring the System Settings

From the above menu, select **Settings...** then select **Client Settings** to display the following window:

Enter the following Information:

Unit Name
Enter a name by which the specific unit can be identified.

Unit Description
(Optional) Enter an additional description if required.

Channel Name (1 and 2)
Entering a specific name for each channel allows easy identification of the door that the channel is managing, as shown in the example.

Server Name
Important: enter here the **IP Address** of the PC that is running the FaceKey Control Centre software.

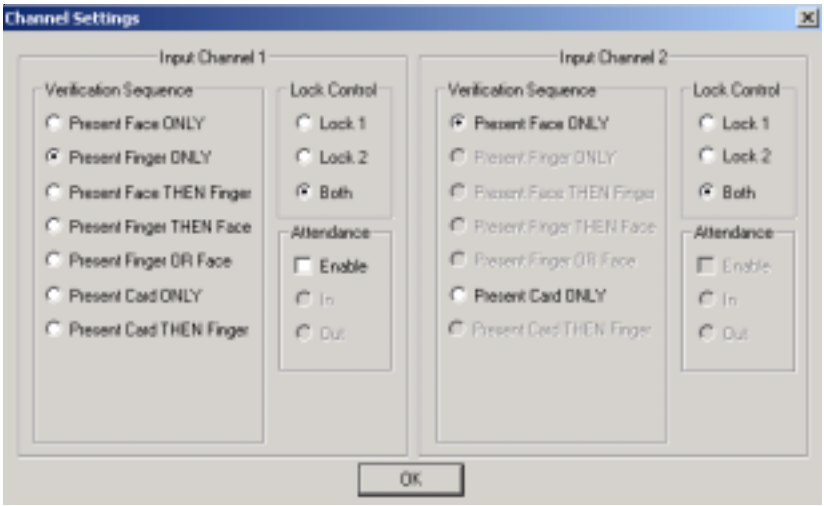
If the server and client software are being run on the same unit the IP address 127.0.0.1 can be used.

Server Port
This is set by default at 9110 but can be changed if required. **Important - the server port set here must match the server port set on the Control Centre software**.

When the fields have been configured as required, click **OK** to exit the dialog box saving any changes that have been made.

Setting the Verification Sequence Options

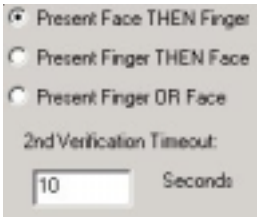
From the client menu, select **Settings...** then select **Verification Sequence** to display the following window:



Depending on what devices are connected to the Access Controller, a variety of verification sequence options can be chosen (for example, if no camera is installed then the face options will be greyed out).

In the *Verification Sequence* field of each channel select the sequence option required for the installation.

If an option has been selected involving more than one device, an extra field will appear at the bottom of the window. Following is an example:



In the **2nd Verification Timeout** text box, enter the length of time that will be allowed after the first verification has been successfully made (in this case face recognition) for the second verification to be made (in this case fingerprint). After this time the first verification will be lost and the system will be waiting for a new sequence to be started. The default timeout is ten seconds.

In the *Lock Control* field, select which of the two output devices are to be used with each channel, either **Lock 1**, **Lock 2** or **Both** - if *Both* is selected, both locks will be activated upon verification from that channel. (see the hardware installation guide to establish which strike or bolt corresponds with which number).

It is also possible to have both channels running with only one door strike or bolt, allowing two way access control on a door. In this scenario set both channels to the same lock number.

Time and Attendance

The controller can also be used as a time and attendance sign-in/sign-out system. If this option is activated, a report

can be printed from the control centre software of when each user signed in and out. To use this option tick the **Enable** box and select if the channel will be for signing in or signing out.

When the fields have been configured as required, click **OK** to exit the dialog box saving any changes that have been made.

Configuring the Door Strike or Bolt

From the client menu, select **Settings...** then select **Access Controller** to display the following window:

The following steps need to be completed:

1. In the **Open Time** box enter a time in seconds for how long the door strike or bolt should remain open once activated.

2. In the **Lock Type** field select the type of lock that the access controller is connecting to (if connecting a Ringdale door strike select **Standard Strike**).

3 In the **Fail Condition** field select whether the lock is designed to **Fail Open** or **Fail Closed**.

4 (Optional and only applies if a pulse door strike is fitted) Tick the **Side Pressure Pulsing** box to allow a pulse strike to re-fire if side pressure is being applied to it when activated - preventing it from being able to release the door (for example if someone is leaning on the door as a fingerprint is presented).

This window also provides override buttons for each lock:

Open - Hold: clicking this button will hold the door strike or bolt in an open position until an authorised user's fingerprint is recognized at which time the device will return to its default status.

Open - Timed: clicking this button will release the door strike or bolt as if an authorised user's fingerprint has been recognised. The device will remain open for the required time as set in the *Open Time* box at the top of the window.

Lock Solid: clicking this button will hold the door strike or bolt in a locked position until an authorised user's fingerprint is recognized at which time the device will return to its default status.

Download Firmware
Caution: This feature should only be used in consultation with our technical support department.

use this button if it becomes necessary to upgrade the firmware on the Access Control board (this is the PCB mounted on the left wall inside the biometric access controller).

This will open up a browser dialog box. Browse to locate the new firmware file, select and click the **Open** button to start the download.

Click the **OK** button to close the window saving the changes that have been made.

The access controller is now ready for operation.

Other Client Menu Options

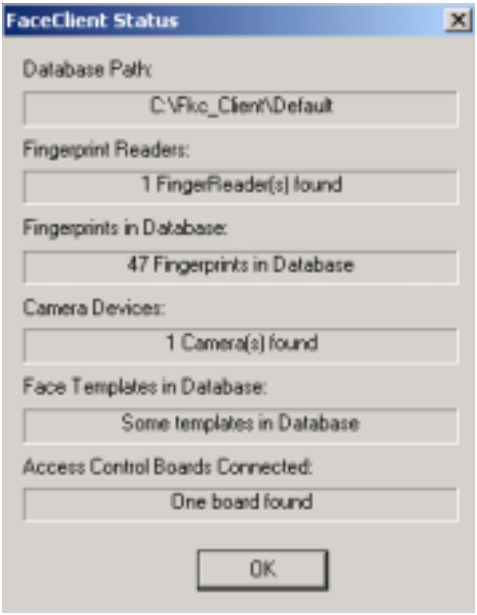
Below are details of additional features that can be accessed from the client menu.

Pause

Select this option to pause the operation of the client software. Once paused, a cross will appear over the FaceKey icon in the bottom right corner of the screen. To restart the client, open the menu again and select the **Resume** option (the client service will need to be paused If making changes to the camera or fingerprint reader sensitivity - see later in the chapter for details of this).

View Status

Selecting this option will display the following window:



This will display the current configuration details of the biometric access controller, including the number of fingerprint readers and camera connected to the unit.

Show...

Selecting this option will display a sub-menu of each channel and allows the monitoring for that channel to be viewed in real time. What is displayed for each channel will depend on the devices running through that channel: fingerprint reader, camera or both. For example, if a camera is connected, the window will display the image from the camera.

Stop Service

The FaceKey client runs as a service on the PC. Selecting this option will stop the client service from running. The FaceKey icon in the bottom right corner of the screen will disappear.

To restart the service, open *Services* on the PC (located in *Control Panel* - exact location will depend on the Windows platform being used). The service will be listed as **FaceKey Client Access Service**. Right click over the name and select *Start*.

Settings...

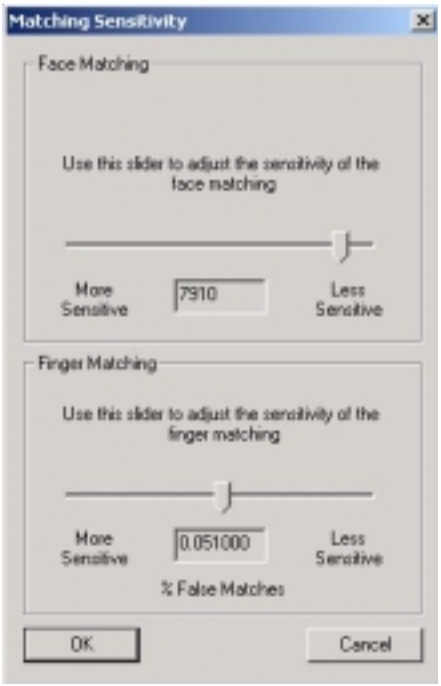
Selecting this option will display the sub-menu shown below:

Following are details of the features that can be accessed from the *Settings* menu:

Client Settings, Verification Sequence and Access Controller
Details for these options can be found in the previous chapter *Configuration Procedures*.

Sensitivity
This option allows the sensitivity of the camera or fingerprint reader to be adjusted. The following window will be displayed:

Important: if making changes to the thresholds settings, it is recommended that the client service is paused while the changes are made (see the start of this chapter for details on pausing and resuming the client).



Face Matching: Use the slider to adjust the camera threshold from more sensitive to less sensitive - because the circumstances for each installation will be different, for example the lighting level will be variable, it might be necessary to make the software less sensitive in darker environments etc.

Important: the more sensitive the slider is set to, the less chance there is of an incorrect acceptance, but this will also make an incorrect rejection more likely. It will be necessary to find a compromise best suited to the specific environment of the installation.

Finger Matching: Fingerprint reader settings are a trade-off between accuracy and useability. The higher the level of accuracy that is set as a requirement, the greater the difficulty there will be in achieving an acceptable reading. By default, the fingerprint reader is set with a false accept threshold of one in ten thousand (the likelihood of an unauthorised fingerprint gaining access).

In certain situations a higher threshold will be required (for example in installations where security is very important). In this scenario the accuracy required for acceptance will be greater, therefore there will be an increased rejection rate for fingers that are not placed cleanly on the reader. The fingerprint reader can be set to a false accept threshold of up to one in one hundred thousand.

In other situations where there is a high level of usage but security is not of paramount importance (the fewer rejections the better) it might be preferable to lower the false accept threshold. The fingerprint reader can be set to a false accept threshold as low as one in one thousand.

Click and hold the pointer on the slider bar and move to the required position.

Click **OK** to save the changes.

Camera...
Selecting this option opens an additional sub-menu of three options as follows:

Portrait Camera: Tick this option to display the camera image in portrait mode. If this is not selected the camera will display in landscape mode. It is recommended that the image is displayed in portrait mode.

Image Settings: This option will link to the property pages of the camera software, allowing the camera to be configured to the requirements of the installation. The information and features displayed here will be dependent on the type of camera that is being used - consult the camera documentation for more details.

Image Size: Selecting this option will display the following window:

These sliders can be used to manipulate the camera image size. This is the image that the software will use to identify an individual.

The smaller the image size is set to, the easier and faster the software will be able to process the data and make an identification. **Note:** Setting the image size is a trade off. The smaller the image size is set to, the closer and more exact the position of the user will have to be in relation to the camera. The bigger the viewing field, the easier it will be for the camera to locate the user. It will be necessary to find a compromise best suited to the specific environment of the installation.

Version 2 Reader Support
Select this option only if using old version 2 fingerprint readers.

Uninstalling the Client Software

Uninstall the Client software as follows:

1 Ensure the Client program is closed.

2 From the **Start** menu select **Settings/Control Panel/Add/ Remove Programs** and select **Access Control** from the list. Click on the **Add/Remove** button and the program will be removed from your PC (If the *Control Centre* and *Client* programs are installed on the same PC this will uninstall both).

Note: before attempting to install a new version of the software it is advisable to reboot the PC.

Ringdale Ltd
56 Victoria Road
Burgess Hill
West Sussex
RH15 9LR
United Kingdom

Freephone: 0800 214503
Tel: +44 (0) 1444 871349
Fax: +44 (0) 1444 870228

Ringdale GmbH
Cochemer Straße 12-14
D-68309 Mannheim
Germany

Freephone: 0800 - 8251880
Tel: +49 (0) 621 7186-0
Fax: +49 (0) 621 7186-20

Ringdale Inc
101 Halmar Cove
Georgetown, Texas 78628
USA

Freephone: 888 288 9080
Tel: +1 512 288 9080
Fax: +1 512 288 7210

Website: http://www.ringdale.com