ACT Enterprise

User Guide

VANDERBILT

Table of Contents

1 About This Documentation

This documentation contains the following information:

- Procedural ("How to") information on common tasks you may want to perform with ACT Enterprise. For more information, see *How To* on page 15.

- Reference material for each of the screens in the four main ACT Enterprise modules.

  See:

  - *ACT Monitor Reference* on page 150
  - *ACT Manage Reference* on page 85
  - *ACT Install Reference* on page 53
  - *ACT ServerClient Reference* on page 48

1.1 Terminology

The following terminology is used throughout:

- Operator / DB User = Person using ACT Enterprise software

- User = Person whose access is managed by the ACT Enterprise software/system

- Installer = Person who installs the physical hardware for the system

- Customer = Company who is benefiting from the ACT Enterprise system

2 General Information

This section describes the following:

2.1 Navigating ACT Enterprise client interfaces

ACT Enterprise client software is designed with common layout characteristics and features. A sample interface is shown below, and the corresponding table describes the numbered features.
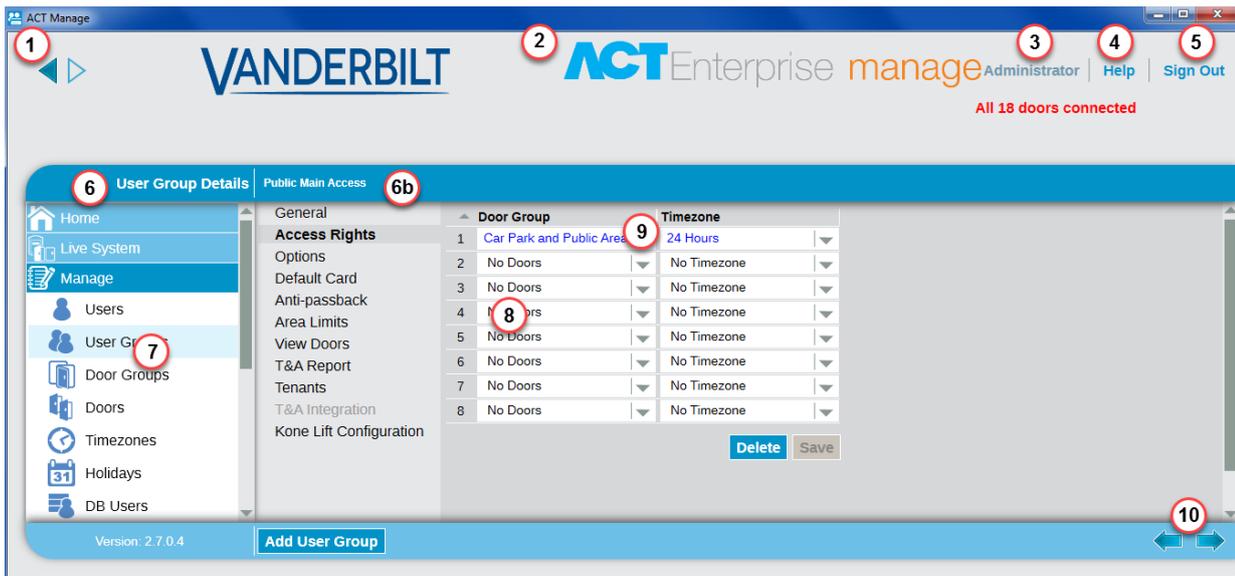
The following table describes each of the navigation features on the screen.

No	Feature	Description
1	Back and Next buttons	These allow you to navigate backwards and forwards between screens already visited.
2	Product name	This shows you which ACT Enterprise module you are currently using.
3	User	This shows which operator (DB User) is currently logged in to the software.
4	Help	This link opens the online help, where you can get more information related to the tasks you are performing.

No	Feature	Description
5	Sign Out	This lets you log out of the current client.
6	Screen name	This label gives the name of the screen you are currently on. The **Home** screen shows quick links to popular tasks.
6b	Sub-screen name	The sub-screen label reflects a specific tab you are on, or an item's name when adding/editing an item, such as a user.
7	Menus	The menus allow you to navigate to particular screens in the software. If a menu has sub-options, when you click the menu name a list of the options appears below it in the menus area and you should click the option you want; if a menu has no sub-options, the screen for the menu item appears in the main area of the screen.
8	Main Screen	This is where the data/settings corresponding to the selected menu item/option are shown.
9	Hyperlinks	If an item in search results is displayed in blue text, it is a hyperlink. Click it to view more detailed information on that item.
10	Page forward () Page back ()	Click to move backwards and forwards through a series of records.

2.2 The Login screen

To log in to your selected ACT Enterprise client software, launch the client and on the login screen enter your username and password.

If Windows authentication/single sign on is enabled for your Windows account in ACT Enterprise, you are logged in to the client automatically using the associated ACT Enterprise DB user account. You do not need to enter a username and password.

If your Windows account is associated with more than one DB user account, you are logged in to the first DB user account found by default. If this is not the correct account, click **Sign out**, then log in again using the correct ACT Enterprise username and password.

If there is a problem connecting to the server, an error with details of the problem is displayed.

Click **Enterprise Server Settings** to access a screen where you can edit/test your connection to the server (see *Enterprise Server Settings* on the facing page).

Click **Change Password** to access a screen where you can change your ACT Enterprise account password. You must enter your current password in order to change it. If you have forgotten your password, ask an ACT Enterprise administrator in your organisation to change your password for you. Passwords should comply with the password policy configured for your organisation. For more information, see *Settings > DB Users Password Policy Tab* on page 148.

2.3 Enterprise Server Settings

The following table describes the data that appears on the **Enterprise Server Settings** screen.

Field Name	Description
Host Name or IP	The name or IP address of the ACT Enterprise server.
Port	The communication port for the ACT Enterprise server.
Test Connection	Click to test the connection to the specified host and port.
	An on-screen message indicates whether the connection succeeded.
	If you edited the server details and want to save the changes, click **Save**. Otherwise, click **Cancel** to return to the login screen.

2.4 About PINs

PINs only need to be assigned for systems requiring Card & PIN or PIN Only usage.

PINs can be set for individuals or for user groups.

If a PIN is set for a user group, it must be unique across all user groups on the system.

If a PIN is set for a user group, the user group's PIN becomes the default PIN for all users in that group, but can be overridden on a user-by-user basis.

If you enter a personal PIN for a user, this overrides the default user group PIN for that user. If you delete an individual PIN for a user, their PIN then reverts to the user group PIN (if set).

You cannot delete a default PIN at the user level.

2.5 Exporting

On a number of screens, you see an **Export** option in the top right-hand corner (**Export**). In this case, the data displayed on the screen may be exported to a CSV (Comma Separated Value) file. The separator character used in the exported file is set on the **Settings > General** tab (see *Settings > General Tab* on page 140).

Click **Export**, and in the dialog that appears specify the required file name and location, then click **Save**. The file may be opened later in a text editor, or a spreadsheet software such as Microsoft Excel.

2.6 Printing

On a number of screens, you see a **Print** option in the top right-hand corner (**Print**). In this case, the data displayed on the screen may be printed using any configured printing device on your local machine.

Click **Print** to open the **Print** dialog for your computer, from which you can select your preferred printer.

2.7 General tips on searching

- When you enter text in a search field, the system searches for both full and partial matches.

  For example, consider searching for a user record using the search term "Ann" in the Name field. A user's name is made up of their first name and last name, and if the specified term appears anywhere in either of these, it is considered a match. So searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**anne** Murphy", and "Joseph H**ann**".

- To sort search results alphabetically by the values in certain columns, click the column title. The first click sorts the information in alphabetic order (A to Z) or numeric order (0-n). Click a second time to sort in reverse-alphabetic order (Z to A) or reverse-numeric order (n-0). Search results can only be sorted by the values in certain columns. Search result descriptions throughout this Help system indicate which data you can use to sort records.

- When sorting search results, if multiple pages of search results are returned, sorting all results returned is limited to user listings only, and only applies for the user name, group number, and user number columns. On other pages and for other values on user listings screens, only the results shown on the current page of search results are sorted.

2.8 The User Lookup screen

The following table describes the search fields available on the **User Lookup** screen.

Field Name	Description
Search	Enter all or part of the registered name for the user whose record you want to view and click the **Search** icon (🔎). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**ann**e Murphy", and "Joseph H**ann**".
Advanced. Click **Advanced** to see the following additional search fields. You can use one or more fields to specify your search criteria.	
User Number	Enter the user number. The system returns an exact match if found.
First Name	Enter all or part of the user's first name.
Last Name	Enter all or part of the user's last name.
Group	Select the group to which the user is assigned.
Card number	Enter the user card number. The system returns an exact match if found.
State	Select the user state: **Enabled**, **Disabled** or **All** (either).
Selectable field	At the final search field, select one additional user field to search on, and enter matching text.

The following table describes each of the columns on the **User Lookup** screen search results area.

Column Name	Description
No	The unique number that identifies this user on the system. (Sortable.)
Name	The user's name. (Sortable.)
Group	The group this user is a member of. (Sortable.)

3 How To

This section describes the following:

3.1 Configuring the system

This section describes how to perform the following system configuration tasks.

3.1.1 Add a controller

ACT Install allows you to configure controller properties, and to specify which doors are connected to that controller.

See also:

- *Adding a controller manually* below

- *Adding a controller using the Add Controller Wizard* on the next page

- *Add an ACT controller and its connected doors using the Autodiscover Wizard* on page 19

Adding a controller manually

1. In ACT Install, click **Advanced Setup > Controllers**, and click **Add Controller** in the top right corner of the **Controllers** screen.

   The **Controller Details** screen displays.

2. Specify details for the new controller.

    For more information on the tabs and fields available on this screen, see *Controller Details* on page 56.

    At a minimum, you must specify:

    - On the **General** tab:
        - A unique **Controller Number**
        - The **Enabled** status
        - The **Controller Type**
    - On the **Communications** tab:
        - The connection type (direct or hubbed), and connection details.
    - On the **Doors** tab:
        - If a door is to be added to the system, select the **In DB** check box and ensure the door is **Enabled**.

3. Click **Save** to add the new controller to the system.

Adding a controller using the Add Controller Wizard

In ACT Install, click **Quick Setup > Add Controller**, or click **Add Controller** on the **Live System** screen to open the **Add Controller Wizard** which walks you through adding one or more new controllers step by step.

- **Step 1: Set Number of Controllers.** Specify the **Number of Controllers** you want to install.

  Click **Next** to continue.

- **Step 2: Controller Details.** Specify the **Controller Name**, **Controller Number**, and **Controller Type**. To enable the controller once added, select the **Enabled** check box.

  Click **Next** to continue.

- **Step 3: Communication Details.** Specify how the controller is connected to the system. There are two options: **Direct to ACT Enterprise** (using TCP/IP or a serial connection), or **Hubbed to Controller** (in this case, the intermediate controller should be specified).

  You can test your communication settings by clicking **Test Connection**.

  Click **Next** to continue.

- **Step 4: Set Doors.** For each door connected to the controller, select the **Enable** check box to enable the door, and select the **In DB** check box to add it to the system.

  Click **Next** to continue.

  Note: If you selected to add more than one controller, the wizard returns to the **Controller Details** screen for the next controller at this point, unless you have specified all controllers, in which case it proceeds to the **Downloading** screen.

- **Step 5: Downloading.** The progress bar and status area indicate how the download is progressing. When the download is complete, click **Next** to continue.

- **Step 6: Validation.** Validate the installed doors by selecting the check box for each door and clicking **Lock**, **Unlock**, **Pass** or **Normal** to issue commands to the selected doors, confirming whether they are connected and responding to commands.

  Click **Next** to continue.

- **Step 7: Finish.** A report on the results of the **Add Controller** wizard.

  Click **Finish**.

3.1.2 Enable/disable controllers

ACT Install allows you to enable/disable controllers individually or in bulk.

Note: Disabling a controller is a way to disconnect that controller from the software, but the controller continues to operate independently unless physically disconnected. Enabling a controller connects it to the system software, but it must be physically connected and accessible on the network.

Enabling/disabling individual controllers

1. In ACT Install, click **Advanced Setup > Controllers**, then use the **Search**/**Advanced Search** options on the **Controllers** screen to find the controller you want to enable/disable.

   For more information on the search options on the **Controllers** screen, see *Controllers* on page 56.

2. Click the name of the controller to view its details on the **Controller Details** screen.

3. On the **General** tab of the **Controller Details** screen, select the **Enabled** check box to enable the controller, or de-select it to disable the controller.

4. Click **Save**.

Enabling/Disabling Multiple Controllers

1. In ACT Install, click **Advanced Setup > Controllers**, then use the **Search**/**Advanced Search** options on the **Controllers** screen to find the controllers you want to enable/disable.

   For more information on the search options on the **Controllers** screen, see *Controllers* on page 56.

2. In the search results, select the check box for each controller you want to enable/disable.

3. Click **Enable** to enable all selected controllers, or click **Disable** to disable all selected controllers.

3.1.3 Add an SPC Panel

Vanderbilt SPC is an intrusion detection platform that delivers a modern, powerful security system. SPC offers versatility with its wired and wireless intrusion components, integrated access solutions, and comprehensive alarm management functionality. Through the use of secure cloud services, a dedicated software suite, and end-user apps, SPC is at the forefront of modern intrusion technology.

ACT Install enables you to configure a connection from ACT Enterprise to an SPC panel. You can monitor and command a connected SPC panel from ACT Enterprise using the ACT SiteMaps tools.

Prerequisites:

- The FlexC plugin must be installed.

- The SPC panel must be installed and configured with an ATS that connects to your installation of ACT Enterprise.

- You must create a custom event profile for use with the ATS. **Zone State Change** events must be enabled for the event profile used by the ATS that connects to your installation of ACT Enterprise.

- The ATP that connects to your installation of ACT Enterprise must have the following settings:

  - **RCT TCP Port** set to **52010**.

  - **RCT URL or IP Address** set to the IP address of the ACT Enterprise server.

  - **Encryption Mode** set to **Auto Encryption** (under **ATP Configuration > Advanced ATP Settings**).

  See the *SPC 4xxx/5xxx/6xxx Installation & Configuration Manual* for more information on configuring an ATS and editing event profiles.

Adding an SPC panel in ACT Enterprise

1. In ACT Install, click **Advanced Setup > SPC Panels**, and click **Add SPC Panel** in the top right corner of the **SPC Panels** screen.

   The **Add SPC Panel** screen displays.

2. Specify the following details for the SPC panel.

   - **Panel Name**: This value will be used to identify the panel in ACT Enterprise.

   - (**Optional**) **Panel Address**: The location of the panel, for example, **London Office**.

   - **Panel Registration ID**: The registration ID for the ATS (alarm transmission system) that connects to ACT Enterprise on the panel. For information on how to find the ATS registration ID for a panel, see *Finding the ATS registration ID of a panel* below.

   - **Panel Connection Information (User)**: Enter the credentials of the panel user account that ACT Enterprise will use to access the panel.

     Note: The panel user account must have **Web Access** enabled.

3. Click **Register Panel** to register the SPC panel with ACT Enterprise.

Finding the ATS registration ID of a panel

1. Log in to the SPC panel embedded web page as a user with Engineer Programming rights.

2. Go to **Communications > FlexC > FlexC ATS**.

   The **Registration ID** for the ACT Enterprise ATS is shown in the **Configured ATS** table.

3.1.4 Add a hub group

A hub group acts as a virtual controller for the management of a group of eLock hubs. Up to four eLock hubs can be connected to a single hub group to share the management of a set of wireless locks. When an eLock connects wirelessly to any eLock hub, that hub shares the information from that eLock with other eLock hubs in the hub group.

ACT Install allows you to add hub groups to the system and to configure properties for their operation.

Add a hub group

1. In ACT Install, click **Advanced Setup > Hub Groups**, and click **Add Hub Group** in the top right corner of the **Hub Groups** screen.

   The **Hub Group Details** screen displays.

2. Specify details for the new hub group.

   For more information on the tabs and fields available on this screen, see *The Hub Group Details screen* on page 60.

3. Click **Save** to add the new hub group to the system.

3.1.5 Add a door

Doors are physical gateways linked to controllers, such as doors, gates, or turnstiles.

ACT Install allows you to add doors to the system and to configure basic properties for their operation.

See also:

- *Add a door manually* on the facing page

- *Add a door using the Add Door Wizard* on the facing page

- *Add a controller* on page 15

- *Add an ACT controller and its connected doors using the Autodiscover Wizard* on the facing page

Add a door manually

1. In ACT Install, click **Advanced Setup > Doors**, and click **Add Door** in the top right corner of the **Doors** screen.

   The **Door Details** screen displays.

2. Specify details for the new door.

   For more information on the tabs and fields available on this screen, see *Door Details Screen* on page 65.

3. Click **Save** to add the new door to the system.

Add a door using the Add Door Wizard

In ACT Install, click **Quick Setup > Add Door**, or click **Add Door** on the **Live System** screen, to open the **Add Door Wizard** which walks you through adding one or more new doors step by step.

- **Step 1: Select Controller.** Select the controller to which the new door should be installed.

  Click **Next**.

- **Step 2: Set Doors.** Select which door(s) to add and enter a description of each door in the **Name** field.

  Click **Next**.

- **Step 3: Download Changes.** Changes are downloaded to the controller. The progress bar and status area indicate how the download is progressing.

- **Step 4: Validation.** Validate the installed doors by selecting the check box for each door and clicking **Lock**, **Unlock**, **Pass** or **Normal** to issue commands to the selected doors, confirming whether they are connected and responding to commands.

  Click **Next** to continue.

- **Step 5: Finish.** A report on the results of the **Add Door** wizard.

  Click **Finish**.

3.1.6 Auto-discover networked controllers

ACT controllers and their connected doors can be automatically detected by ACT Install.

Add an ACT controller and its connected doors using the Autodiscover Wizard

1. In ACT Install, click **Quick Setup > Autodiscovering**, or click **Advanced Setup > Controllers**, then click **Autodiscover**.

   The **Autodiscover Wizard** opens. This wizard walks you through adding one or more new controllers plus connected doors step by step.

   Note: The **Autodiscover Wizard** can only detect ACT controllers that are connected to the network. Other controllers should be added manually (see *Adding a controller manually* on page 15), or using the Add Controller Wizard (see *Adding a controller using the Add Controller Wizard* on page 16).

2. Follow the wizard's onscreen instructions to add and configure a new controller and its connected doors, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

   Please see below for notes relevant to the **Hardware Review** step in the wizard.

3.1.6.1 Notes on Hardware Review

During the **Hardware Review** step, the Autodiscover Wizard reports on:

- **Database:** ACT controllers already in the database and online

- **New:** ACT controllers detected on the LAN that are not currently in the database.

- **Missed:** ACT controllers in the database but not found and new ACT controllers found that aren't already in the database

- A warning is given if multiple controllers are found to have the same number (id).

3.1.7 Test controllers/doors

ACT Install allows you to remotely test controllers and doors using the Validation Wizard. The Validation Wizard sends specified commands to controllers/doors on the network and validates their responses to determine whether or not they are functioning correctly.

Testing controllers/doors

1. In ACT Install, click **Tools > Validation Wizard**.

   The **Validation Wizard** appears.

2. Select the controllers/doors to be validated and click **Next**.

3. Select which commands to test during validation (Door Lock, Door Unlock, Door Pass, Door Normalize) and click **Next**.

   ACT Install validates the selected hardware and commands, and displays a report which indicates whether or not each test was successful.

   Note: "Success" means the command could be issued. The result of the test on the hardware has to be separately assessed. That is, if you command a door to lock, the software reports whether the lock command was issued. To validate that the door was actually, physically locked, then you must check the door itself.

4. Review the report, take note of any hardware that failed validation so that you can investigate and repair or replace as appropriate, then click **Next**.

   ACT Install displays a summary of the test results.

5. Click **Finish**.

3.1.8 Check the system status

There are a number of ways to check the status of your ACT Enterprise system.

- In ACT Install, click **Live System** to see the status of all configured controllers, doors, and I/O modules on the system, and to view live information on events occurring across the system.

  For more information, see *Live System (ACT Install)* on page 53.

- In ACT Install, click **Reports > System Status** to see a quick summary of the statuses of controllers, doors and I/O modules on the system. This report can be printed or exported using the links at the top-right corner of the screen.

  For more information, see *System Status* on page 79.

- In ACT Install, click **Reports > System Snapshot** to see a list of all controllers, doors and I/O modules with summary information about each device and its current status, and also a list of recent system events. This report can be printed or exported using the links at the top-right corner of the screen.

  For more information, see *System Snapshot* on page 79.

3.1.9 Set properties for multiple doors

If you want to set a property for multiple doors, ACT Install allows you to do this in bulk instead of editing each door individually.

Setting properties for multiple doors

1. In ACT Install, click **Advanced Setup > Doors**, then use the **Search/Advanced Search** options on the **Doors** screen to find the doors for which you want to set properties.

For more information on the search options on the **Doors** screen, see *Doors Screen* on page 64.

2. In the search results, select the check box for each door for which you want to set properties.

3. Click **Bulk Properties**.

The **Door Options Wizard** appears.

Note: The properties displayed are the system defaults and do not reflect the current values on the selected controllers. Only selected properties are downloaded.

- **Step1: Select Options.**

  - On the **Timers** tab, set the required timer values

  - On remaining tabs, set the required properties to enable/disabled:

    - Click the lock icon to lock ( ) or unlock ( ) an option.

      The enabled/disabled settings for unlocked options are applied to the selected doors; the settings for locked options are ignored.

    - For timers, enter a time in seconds that the corresponding output is activated when it is fired.

    - Select the check box for an option to mark it as enabled for all selected doors, or leave the check box de-selected for an option to mark it as disabled for all selected doors.

  - Click **Next**.

- **Step 2: Verify Options.** This screen itemises the enabled/disabled settings the wizard will apply to the selected doors. Review the details carefully before proceeding. If any settings are incorrect, click **Back** to return to the previous screen and amend them.

  Note: There is no **Undo** option.

  If you are satisfied that the options are all correct, click **Next**.

- **Step 3: Downloading.** ACT Install applies the enabled/disabled options to the selected doors. A progress bar indicates how the download is progressing.

- **Step 4: Finish.** Once all settings have been applied, the **Finish** screen summarises the changes made.

  Click **Finish** to return to the **Doors** screen.

3.1.10 Set properties for multiple controllers

If you want to set a property for multiple controllers, ACT Install allows you to do this in bulk instead of editing each controller individually.

Setting properties for multiple controllers

1. In ACT Install, click **Advanced Setup > Controllers**, then use the **Search**/**Advanced Search** options on the **Controllers** screen to find the controllers for which you want to set properties.

   For more information on the search options on the **Controllers** screen, see *Controllers* on page 56.

2. In the search results, select the check box for each controller for which you want to set properties.

3. Click **Bulk Properties**.

The **Controller Options Wizard** appears.

4. For each tab (**Door 1 Options**, **Door 2 Options**, **Operations - General**, **Operations - ACT1000**, and **Operations - Printer**), set the required properties to enable/disabled:

   a. Click the lock icon to lock (![lock]) or unlock (![unlock]) an option.

      The enabled/disabled settings for unlocked options are applied to the selected controller; the settings for locked options are ignored.

   b. Select the check box for an option to mark it as enabled for all selected controllers, or leave the check box de-selected for an option to mark it as disabled for all selected controllers.

      Note: The check box does not reflect the actual value currently on the controllers.

5. Click **Next**.

   The **Verify Options** screen displays itemising the enabled/disabled settings the wizard will apply to the selected controllers. Review the details carefully before proceeding. If any settings are incorrect, click **Back** to return to the previous screen and amend them.

6. If you are satisfied that the options are all correct, click **Next**.

7. ACT Install applies the enabled/disabled options to the selected controllers. A progress bar indicates how the download is progressing.

8. Once all settings have been applied, the **Finish** screen summarises the changes made.

   Click **Finish** to return to the **Controllers** screen.

3.1.11 Change database

The ACT Enterprise database contains details of all your controllers, doors, I/O modules, users, user groups, etc. You can connect to an alternative database.

Before connecting to an alternative database:

- Carefully consider the implications of connecting to an alternative database. This is not something to be undertaken without serious consideration.

- Ensure that your new database is structured correctly. For information on creating a new (empty) database and migrating data to it from an existing database, see the following topics:

  - *Add a new database* on the facing page
  - *Migrate a database* on page 24

Changing to a SQL Server database

1. In ACT ServerClient, click **Database**.

   The **Database** screen displays the details of the currently connected database.

2. Click **Change Database**.

   The **Change Database** dialog appears.

3. Configure the new database details:

   a. From the **Server name** drop-down list, select the name of the server that is hosting your SQL Server.

   b. At **Log in to the server**, select your authentication method.

      If you select **Use Windows Authentication**, you should ensure that your SQL database allows access from the Local System account on the ACT Enterprise server.

      If you select **Use SQL Server Authentication**, specify a valid **User name** and **Password**. The user name and password are passed explicitly to the SQL Server: confirm that this is acceptable with your system administrator. Remember that if the user name and password change, you must re-enter them here.

      c.   At **Connect to a database**, select the database that you want to connect to from the **Select or enter a database name** drop-down list.

      d.   Click **Test Connection** to verify that ACT Enterprise can connect to the database.

4. Click **OK**.

Changing to a SQL Compact database

1. In ACT ServerClient, click **Live System > Stop** to stop the ACT Enterprise service.

2. In Windows Explorer, navigate to the following folder:

   C:\ProgramData\Access Control Technology\ACT Enterprise\Database

3. (**Optional**) If you are currently using a SQL Server database, you must remove connection details from the ActEnterpriseDatabase.txt file.

   To do this, delete the contents of ActEnterpriseDatabase.txt and save it as a blank file.

4. Rename the ActEnterprise.sdf database file. For example, name it ActEnterprise_OLD.sdf.

5. Copy your new SQL Compact database file to this folder and rename it ACTEnterprise.sdf.

6. In ACT ServerClient, click **Live System > Start** to start the ACT Enterprise service.

3.1.12 Add a new database

The ACT Enterprise database contains details of all your controllers, doors, I/O modules, users, user groups, etc.

You can create a new database for ACT Enterprise at any time.

For information on migrating data from another database to your new database, see *Migrate a database* on the next page.

Creating a new SQL Server database

1. In ACT ServerClient, click **Database**.

   The **Database** screen displays, showing details of the currently connected database.

2. Click **Create Database** to create a new database.

   The **Add New Database** dialog appears.

3. For ACT Enterprise, the **Data source** is always **Microsoft SQL Server** – do not change this setting.

4. From the **Server name** drop-down list, select the name of the server hosting your SQL Server.

5. At **Log in to the server**, select your authentication method.

   If you select **Use Windows Authentication**, you should ensure that your SQL database allows the Local System account to access it from the server ACT Enterprise runs on.

   If you select **Use SQL Server Authentication**, specify a valid **User name** and **Password**. The user name and password are passed explicitly to the SQL Server, so you should verify this is acceptable with your system administrator. In addition, if the user name and password change, then you must re-enter them.

6. At **Connect to a database**, enter the name of your new database in the **Select or enter a database name** field.

7. Click **OK**.

Creating a new SQL Compact database

1. Stop the ACT Enterprise service.

   To do this, in ACT ServerClient, click **Live System > Stop**.

2. In Windows Explorer, navigate to the following folder:

    C:\ProgramData\Access Control Technology\ACT Enterprise\Database

3. Rename the database file ActEnterprise.sdf. For example, name it ActEnterprise_OLD.sdf.

4. Make a copy of the ACTEnterprise_Blank.sdf database file and rename it to ACTEnterprise.sdf.

5. Start the ACT Enterprise service.

    To do this, in ACT ServerClient, click **Live System > Start**.

3.1.13 Migrate a database

The ACT Enterprise database contains details of all your controllers, doors, I/O modules, users, user groups, log events, and so on.

If you have a legacy database, ACT Enterprise can migrate information from that database to a database in the currently supported format. During migration, the following actions are performed:

- The destination database is cleared down and repopulated with data from the source database.

- Log events outside of the specified range are purged.

- Large user images are downsized.

Prerequisites:

- Create a backup of your source database.

- Create a new, empty ACT Enterprise database to use as a target for the migration.

    For information on how to create a new ACT Enterprise database, see *Add a new database* on the previous page.

- Ensure that ACTWin pro and the ACT Enterprise service are not running.

    To stop the ACT Enterprise service, in ACT ServerClient, click **Live System > Stop**.

Migrating a database

1. In ACT ServerClient, click **Database**.

    The **Database** screen displays, showing details of the currently connected database.

2. Click **Migrate Data**.

3. Click **Yes** to confirm that you want to perform a migration.

    Migration will overwrite all existing data in the target database.

    The **Migrate Legacy ACT Data** dialog appears.

4. Enter details for the source database. To do this:

    a. Under **Source Database Type**, select the type of the legacy database.

    b. For a **Jet/Access** or **SQL Compact** database, click **Browse** to open a dialog where you can browse to and select the database file.

    c. For a **SQL Server**, click **Browse** to open a dialog where you can configure database connection properties, including server name and authentication details.

5. Enter details for the destination database. To do this:

    a. Under **Destination Database Type**, select the type of the target database.

    b. For a **SQL Compact** database, click **Browse** to open a dialog where you can browse to and select the database file.

    c. For a **SQL Server**, click **Browse** to open a dialog where you can configure database connection properties, including server name and authentication details.

6. Under **Migrate Log Events**, select the timeframe for which you want to migrate log events recorded

in the source database.

If you select **Custom**, use the date picker to specify the earliest date from which you want to migrate log events.

7. Click **Start** to begin the database migration.

    You are warned that migrating data deletes everything in the destination database.

8. Click **OK** to proceed.

    A message indicates whether the migration was successful, and the location of the log file for the migration displays.

9. If ACT Enterprise is not already configured to use the destination database, change the ACT Enterprise database. For more information, see *Change database* on page 22.

10. To restart the ACT Enterprise service, in ACT ServerClient, click **Live System > Start**.

11. Verify that the system, user and log information migrated successfully by spot-checking data using ACT Install and ACT Manage.

3.1.14 Change the default service port

In rare circumstances, you may need to change the default service port for ACT Enterprise, for example, if another service is using the same port. In this case, you must reconfigure the service port for ACT Enterprise on the server, and update the service port in ACT ServerClient and in each client you use to connect to the service.

Change the service port in ACT ServerClient

1. In ACT ServerClient, on the **Live System** screen, click **Stop** to stop the service.

2. On the Windows server hosting ACT Enterprise:

    a. Use a text editor to open the following file:

        C:\Program Files\Access Control Technology\ACT Enterprise\ActEnterpriseWinServiceHost.exe.config

    b. Change the value of the **WCFBasePort** parameter to an available port on the Windows machine. You will need up to 11 contiguous available ports starting at the base port, depending on how ACT Enterprise is configured, e.g. 9000, 9001, 9002, …, 9010.

3. In ACT ServerClient, on the **Live System** screen, click **Start** to start the service.

    Wait until the **Service State** is **Running**.

4. In ACT ServerClient, on the **Live System** screen, enter the new **Service Port**, as specified by the **WCFBasePort** parameter, and click **Reconnect**.

    ACT ServerClient connects to the ACT Enterprise service.

Change the service port in ACT Enterprise clients

1. Launch the client (ACT Install, ACT Manage or ACT Monitor).

2. At the bottom of the **Login** screen, click **Enterprise Server Settings**.

3. On the **Enterprise Server Settings** screen, enter the new service port number in the **Port** field and click **Test Connection**.

    If the server address and port provided are correct, and the service is running, the connection will succeed.

4. Click **Save**.

3.1.15 See what hardware is on the network

You can generate a report that provides a snapshot of all hardware on your network from ACT Install.

In ACT Install, click **Reports > System Snapshot** to see a list of all controllers, doors and I/O modules with summary information about each device and its current status, and also a list of recent system events. This report can be printed or exported using the links at the top-right corner of the screen.

For more information, see *System Snapshot* on page 79.

Alternatively, go to **Advanced Setup** and choose what type of hardware you want to review. You can list doors, controllers, IO Modules, DVRs, and cameras.

3.1.16 Configure timers

See also:

- *Configuring timers for a door* below
- *Configuring an input timer* below
- *Configuring an output timer* on the facing page

Configuring timers for a door

1. In ACT Install, click **Advanced Setup > Doors**, or in ACT Manage, click **Manage > Doors**.

2. Using the **Search/Advanced Search** options on the **Doors** screen, find the door for which you want to configure timers.

   For more information on the search options on the **Doors** screen in ACT Install, see *Doors Screen* on page 64.

   For more information on the search options on the **Doors** screen in ACT Manage, see *The Doors screen* on page 104.

3. In the search results area on the **Doors** screen, click the name of the door you want to configure.

   The **Door Details** screen displays.

4. In ACT Install, on the **Timers** tab, you can specify the following timers: **Relay Timer**, **AUX Output**, **OP2 Timer**, **OP3 Timer**, **Door Ajar Timer**, **Extended Relay Timer**, **Tracking Delay Timer**.

   For more information, see *Door Details > Timers Tab* on page 66.

   Or

   In ACT Manage, on the **General** tab, you can specify values for the **Relay Timer** and the **Door Ajar Timer**.

   For more information, see *Door Details > General Tab* on page 105.

5. Click **Save**.

Configuring an input timer

1. In ACT Install, click **Advanced Setup > I/O Modules;** on the **I/O Modules** screen click the **Inputs** link for the I/O module with the input whose timer you want to configure; then on the **Inputs** screen, click the name of the specific input whose timer you want to configure.

   Or

   In ACT Manage, click **Manage > Inputs**, search for the input whose timer you want to configure, and in the search results area on the **Inputs** screen, click the name of the input you want to configure.

   The **Input Details** screen displays.

2. On the **General** tab, in the **Timer** field, specify the amount of time in seconds that the input must remain in a certain state before the change is reported. This prevents a momentary change in the input from causing a false alarm.

3. Click **Save**.

Configuring an output timer

1. In ACT Install, click **Advanced Setup > I/O Modules;** on the **I/O Modules** screen click the **Outputs** link for the I/O module with the output whose timer you want to configure; then on the **Outputs** screen, click the name of the specific output whose timer you want to configure.

   Or

   In ACT Manage, click **Manage > Outputs**, search for the output whose timer you want to configure, and in the search results area on the **Outputs** screen, click the name of the output you want to configure.

   The **Output Details** screen displays.

2. On the **General** tab, in the **Timer** field, specify the amount of time in seconds that the output must remain in a certain state before the change is reported. This prevents a momentary change in the output from causing a false alarm.

3. Click **Save**.

3.2 Managing the system

This section describes how to perform the following system management tasks.

3.2.1 Add a door group

Door groups are a convenient way of grouping a number of doors to simplify granting/denying access to that group of doors. Door groups are essential for applying user group access rights. You must also configure a door group containing designated lockdown doors if you want to use the lockdown feature in ACT Enterprise. For more information, see *Configure and implement system lockdowns* on page 33.

ACT Manage allows you to create and edit door groups. Doors must be added to the system through ACT Install before they can be assigned to door groups. For more information, see *Add a door* on page 18. Any given door may belong to multiple door groups.

See also:

- *Add a door group through the Door Group Details screen* below
- *Add a door group using the Door Group Wizard* on the next page

Add a door group through the Door Group Details screen

1. In ACT Manage, click **Manage > Door Groups**, then click **Add Door Group** in the top right corner of the **Door Groups** screen.

   The **Door Group Details** screen displays.
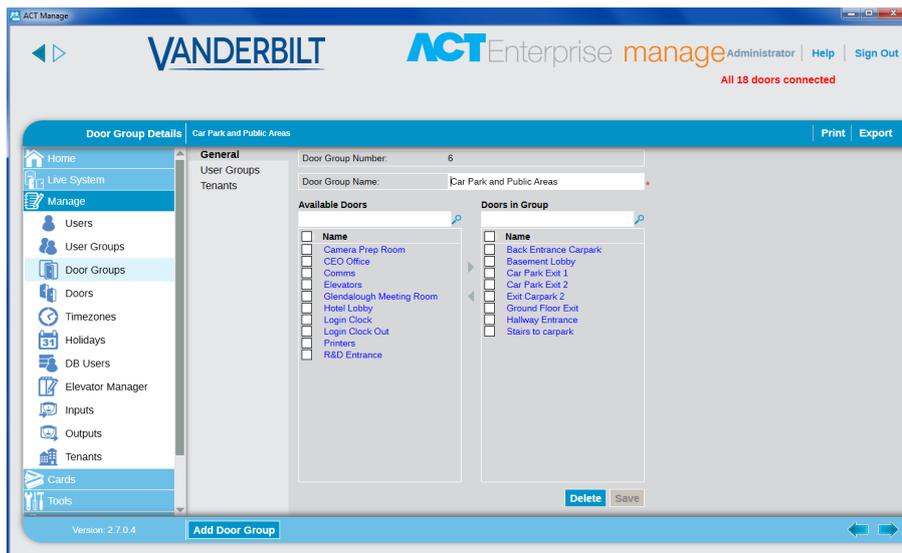
2. Specify the **Door Group Number** and **Door Group Name** on the **General** tab.

3. Specify the doors in the door group on the **General** tab:

   - To add a door, select the door in the **Available Doors** list, then click the right-arrow (▶).

   - To remove a door, select it in the **Doors in Group** list and click the left-arrow (◀).

4. If tenancies are in use, you can select which tenancies this door group is available to on the **Tenants** tab.

   For more information on tenancy, see *Tenancy* on page 121.

5. Click **Save** to create a record for the door group.

Add a door group using the Door Group Wizard

1. In ACT Manage, click **Add Door Group** on the **Home** screen to open the **Add Door Group Wizard** which walks you through adding a door group step by step.

2. Follow the wizard's onscreen instructions to add a new door group, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

3.2.2 Configure operator access rights

ACT Manage allows you to configure operators (also called DB Users) of ACT Enterprise software through the **DB Users** screen. An operator is a person who uses the ACT Enterprise software. You can restrict an operator's access to particular data and functions when using the software.

Note: Only ACT Enterprise administrators can view or change DB users.

Configuring operator access rights

1. In ACT Manage, click **Manage > DB Users**.

2. To edit access rights for an existing operator, click their name.

   The **DB User Details** screen displays.

   For more information on this screen, see *The DB User Details screen* on page 113.
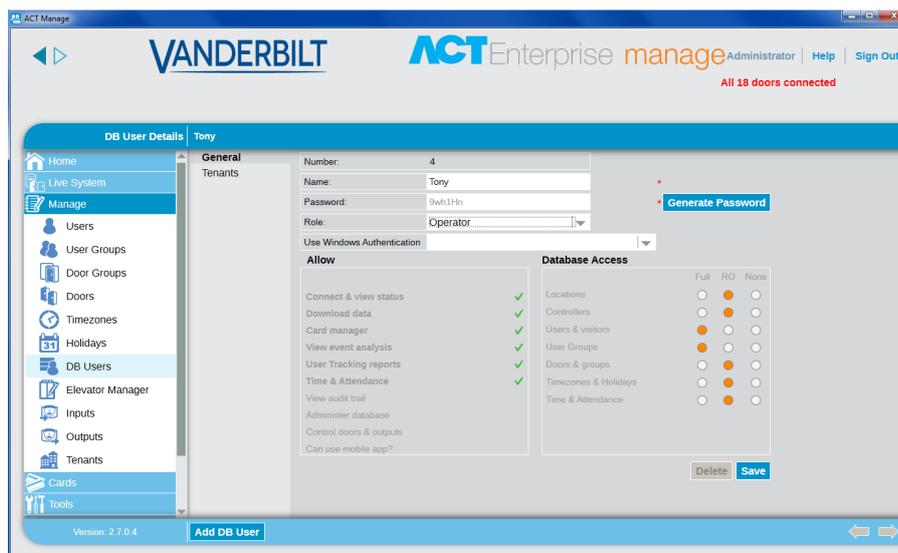
3. From the **Role** drop-down list:

    - Select a standard role to assign the operator a pre-defined combination of rights to access functions and data.

      The **Allow** and **Database access** areas reflect the rights for the selected role.

      Or

    - Select **Custom** to specify a customised combination of rights.

      When you select **Custom**, you can optionally select which clients (**Monitor**, **Manage**, **Install**) the operator should have access to. The appropriate rights are assigned by the system to allow the DB User to access the selected clients.

      Alternatively, select the user's required rights from the **Allow** and **Database Access** areas.

4. Click **Save**.

Note: If a user does not have sufficient minimum access rights for a client, such as ACT Monitor, then the client is disabled in the **Clients** menu.

3.2.3 Enable mobile app support

The ACT Enterprise mobile app can be used to monitor and command the system from Android and iOS devices. DB users can use the app to:

- Generate muster reports, and log users out

- Enable/disable card holders

- Change user photos

- View all recent log events, log events per user, and log events per door

- Command doors and monitor door statuses

To enable app support for your ACT Enterprise system, an ACT Enterprise administrator must:

- Enable mobile access in ACT Manage.

- Grant mobile app rights to authorised DB users. DB users with the **Administrator** role automatically have mobile app rights.

Each authorised DB user should then install and configure the mobile app.

These steps are described in detail below.

Prerequisites:

- ACT Enterprise must be able to connect to the internet to support connections from the mobile app.
- Your ACT Enterprise installation must enforce a strong password policy for DB users. You can enable a strong password policy in ACT Manage under **Settings > DB Users Password Policy**.

Enable mobile access in ACT Monitor

1. In ACT Manage, click **Settings > Mobile Access**.

2. On the **Mobile Access** screen, select the **Enable** check box.

   Note: This check box is disabled if a strong password policy is not enabled under **Settings > DB Users Password Policy**.

3. (Optional) Enter a **Site Description**. This will display on the mobile app interface.

4. Take note of the system-generated **Unique Identifier**. Authorised DB users must enter this identifier in the ACT Enterprise mobile app to access the system.

5. Restart the ACT Enterprise service. To do this, in ACT ServerClient, click **Live System > Restart**.

Grant system access through the app to a DB user

1. In ACT Manage, click **Manage > DB Users**, then click the **Name** of the DB user to whom you want to grant access.

2. On the **DB User Details** screen, select the check box for **Can use mobile app?** in the **Allow** list.

   Note: A DB user can only use the app to carry out functions for which they have rights. For more information on configuring DB user permissions, see *Configure operator access rights* on page 28.

3. Provide the system-generated **Unique Identifier** from the **Settings > Mobile Access** screen to the DB user.

Install and configure the mobile app

1. Download the ACT Enterprise app to your Android or iOS device. The app is available on Google Play and the App Store.

2. Run the app on your mobile device.

3. The first time you run the app, accept the terms of service, enter the **Unique Identifier** provided by your ACT Enterprise administrator, then click **OK**.

   The unique identifier is used to verify which ACT Enterprise system you are connecting to.

4. Enter your ACT Enterprise username and password, then click **Login**.

   You can now monitor and manage the ACT Enterprise system from the app.

3.2.4 Synchronise controller information

The System Synchronise Wizard in ACT Manage and ACT Install allows you to download the entire database to one or more controllers. Controllers remain offline during downloads, meaning that they cannot be commanded during this time, nor can they report events. Door stations have limited functionality during the download. You should only do a download if you are certain it is required.

Note: Synchronising controllers means that all data entered on the controller directly, via its keypad, are lost.

Synchronising controller information

In ACT Manage or ACT Install, click **Tools > System Synchronise**.

The **System Synchronise Wizard** appears.

- **Step 1: Controllers.** This screen indicates whether each controller is up to date or not.

  Select which controllers you want to download to, then click **Next**.

- **Step 2: Downloading.** This screen shows a progress bar which indicates the overall progress of the system synchronisation. The message area shows information for each controller as data is downloaded.

  When the download has fully completed, click **Next**.

- **Step 3: Results.** This screen shows the results of the synchronisation operation: the number of controllers updated and their current statuses.

Click **Finish** to leave the wizard.

3.2.5 Configure door actions

Actions are settings automatically applied by a door controller at specified times without the need for user intervention.

For example:

- A door may require additional security out of office hours where a PIN may be required.

- A door may be set to have card and PIN access 24 hours. This is common for rooms that require a high level of security.

- A door may be automatically opened during business hours.

Actions may be used to control external devices via the controller outputs, or to alter the security level of a door at certain times. Each action may be inactive (default) or have any defined time zone assigned.

Note: Before configuring a door's actions, you should ensure you have created all the time zones required. For more information, see *Add a time zone* on page 33.

Configuring a door's actions

1. In ACT Manage, click **Manage > Doors**. If the door whose actions you want to configure is not immediately visible, use the **Search**/**Advanced Search** options on the **Doors** screen, find the door for which you want to configure actions.

   For more information on the search options on the **Doors** screen, see *The Doors screen* on page 104.

2. In the search results area on the **Doors** screen, click the name of the door you want to configure.

   The **Door Details** screen displays.

3. Click the **Actions** tab of the **Door Details** screen.

4. For each listed action, select a time zone from the corresponding drop-down list to determine when the action applies for this door.

   For a description of each of the available actions, see *Door Details > Actions Tab* on page 105.

5. Click **Save** when you have finished configuring required action/time zone combinations.

Note: Some timed actions are mutually exclusive. In this case, only one timed action should be selected where the times zones overlap. Examples are: **Lock Door** and **Unlock Door**; or **PIN Required**, **PIN or Card**, and **Any Card**.

3.2.6 Configure fire doors

Fire doors are automatically opened if there is a fire event, to allow free passage of users. In ACT Enterprise, fire doors are specified by adding them to a door group, then marking that door group as the one containing **Fire override doors**.

To set up fire doors:

1. In ACT Install, add the controllers and connected doors to the system.

   For more information, see *Add a controller* on page 15 and *Add a door* on page 18.

2. Physically wire your infrastructure so that a common 0V output from the fire panel is brought separately to the AUX input on door 1 of each controller. Each controller that receives the fire event signal automatically unlocks the assigned fire doors and normalises the doors immediately once the fire event is cancelled.

3. In ACT Manage, create a door group for fire doors, and specify which doors are opened automatically in the case of a fire. For more information, see *Add a door group* on page 27.

4. In ACT Manage, specify that this door group is the one containing **Fire override doors**. See below.

Marking a door group as one containing Fire Override doors

1. In ACT Manage, click **Settings**.

2. On the **Settings** screen, click the **Doors** tab.

3. At **Fire override doors**, select the door group containing fire doors.

4. Click **Save**.

3.2.7 Configure holidays

ACT Manage allows you to specify up to 9 holiday types (see *Configuring holiday types* below), and to assign at most one holiday type to each day of the year (see *Marking days of the year as holidays* below).

When you specify time zones (periods when access rights apply), you can mark them as active for week days and also for days assigned specific holiday types. For more information on specifying time zones, see *Add a time zone* on the facing page.

Configuring holiday types

1. In ACT Manage, click **Settings**.

2. Click the **Holiday Names** tab.

3. Enter names for up to nine holiday types and click **Save**.

Marking days of the year as holidays

1. In ACT Manage, click **Manage > Holidays**.

   The **Holidays** screen shows a 12 month calendar starting at the current month, and a list of colour-coded holiday types.

   The current date is selected by default.

   Dates flagged as holidays are highlighted in the corresponding holiday type colour.

   Note: Adding a holiday for a specific day/month combination leaves that holiday for that date in the system for each subsequent year. You should periodically review your holidays, for instance moving bank holidays.

   For more information, see *The Holidays screen* on page 112.
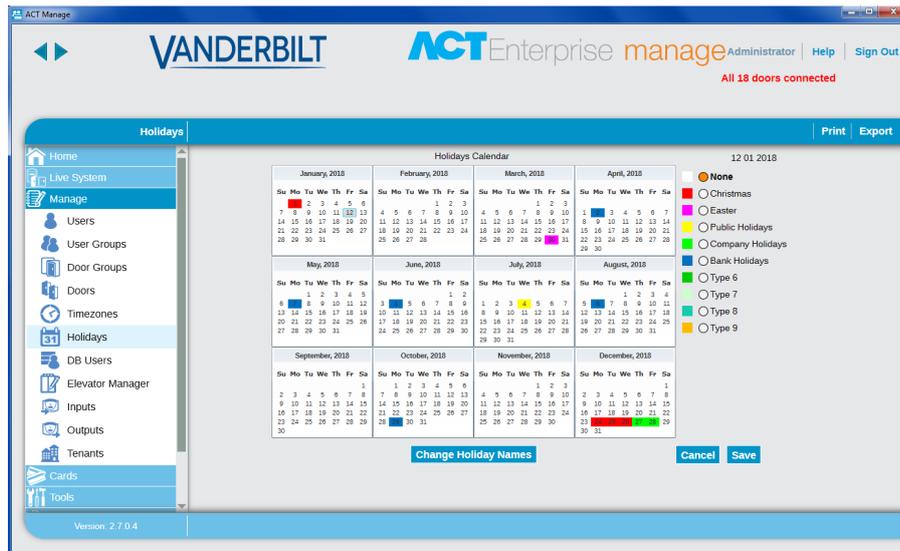
2. To assign or change the holiday type for any date, select that date and click the radio button for a holiday type to assign that type. Only one holiday type may be assigned to each date.

3. To remove a holiday type for any date, select that date and click the **None** radio button.

4. Click **Save**.

3.2.8 Add a time zone

A time zone consists of up to 8 time periods. Each period specifies a time range and the days and holidays for which the period is active. The time zone is active when any of its periods are active.

Time zones are used to specify when a user/group's access rights are valid.

Time zones can be created and edited in ACT Manage.

Adding a Time Zone

1. In ACT Manage, click **Add Time Zone** on the **Home** screen, or click **Manage > Time Zones**, then click **Add Time Zone** in the top right corner of the **Time Zones** screen.

   The **Time Zone Details** screen displays.

2. Enter the **Timezone Name** on the **General** tab.

3. In the lower section of the **General** tab, specify the **Times**/**Days** combinations when this time zone is active.

   To specify a **Times**/**Days** combination, select a row, and in the fields below specify the corresponding **Period** (**From** and **To** times), and select the **Days** and **Holidays**.

4. If tenancies are in use, you can select which tenancies this time zone is available to on the **Tenants** tab.

   For more information on tenancy, see *Tenancy* on page 121.

5. Click **Save** to create the time zone.

3.2.9 Configure and implement system lockdowns

ACT Enterprise can be configured to handle lockdown situations. If lockdowns are enabled, you can set conditions to determine how the system behaves during lockdown: which doors lock, and the conditions under which a locked door opens. During a lockdown, designated doors are locked, preventing access, in response to an emergency. A lockdown overrides any timed actions active on locked doors.

Lockdowns can be initiated from designated card readers by users with the **Lockdown** right, or from the ACT Manage and ACT Monitor clients.

Enabling and configuring lockdowns

1. In ACT Manage, click **Settings > Lockdown**.

2. Select the **Enable Lockdown** check box.

3. From the **Lockdown Doors** drop-down list, select the door group with the doors to lock during a lockdown event.

4. Enable/disable the check box for each lockdown option to determine how the system behaves during lockdown.

   For a description of each of the available options, see *Settings > Lockdown Tab* on page 142.

5. Click **Save** when you have finished configuring lockdown settings.

Giving a card holder rights to initiate and clear a lockdown from a reader

1. In ACT Install, configure the door readers from which a lockdown can be initiated and cleared. To do this, select the **Lockdown Reader** check box under **Door Security** on the **Advanced Setup > Doors> Door Details > Operations** tab.

2. In ACT Manage, create or edit a user group to grant users in that group the right to initiate and clear a lockdown. To do this, select the **Lockdown** check box on the **Manage > User Groups > User Group Details > Options** tab.

3. In ACT Manage, assign each appropriate user to the user group with the **Lockdown** right. To do this, select the **User Group** on the **Manage > Users > User Details > General** tab.

4. In ACT Manage, assign a card to each user with the **Lockdown** right. To do this, click a card icon on the **Manage > Users > User Details > General** tab and follow the instructions on screen. For more information, see *The Card Add screen* on page 96.

Ensure that users with the **Lockdown** right know:

- Your organisation policy on lockdowns

- Which readers are designated lockdown readers

- How to initiate and clear a lockdown using their card

Initiating and clearing a lockdown from a card reader

Once lockdowns have been enabled and configured, a user with the **Lockdown** right can initiate and clear lockdowns by presenting their card at a designated lockdown reader.

- To initiate a lockdown, a user with the **Lockdown** right should present their card once at a designated lockdown reader.

- To clear a lockdown, a user with the **Lockdown** right should present their card twice in rapid succession at a designated lockdown reader.

Initiating and clearing a lockdown from ACT Enterprise

Once lockdowns have been enabled and configured, you can initiate and clear lockdowns from the ACT Manage **Live System** screen and the ACT Monitor **Home** screen:

- To initiate a lockdown, click **Lockdown** on the **Live System** screen. All doors in the door group specified under **Lockdown Doors** on the **Settings > Lockdown** tab in ACT Manage are locked down. A red padlock symbol ( ) displays beside these doors in the **Live System** view.

- To clear a lockdown, click **Clear Lockdown** on the **Live System** screen. All doors return to their previous state.

3.3 Managing users

This section describes how to perform the following user management tasks.

3.3.1 Add a user

A user is a person who holds an access control token (card, fob, PIN, biometric, etc.) and whose access is managed through the ACT Enterprise software.

You can add and edit users through ACT Manage.

When you add a user, you can specify profile details such as their name, user group, validity period, PIN numbers (if applicable) and card details.

See also:

- *Adding a permanent user* below
- *Adding a temporary user* on the next page – Fewer details are specified for temporary users, making setup quicker.
- *Copying an existing user* on the next page

You can specify a validity period for both permanent and temporary users – this allows you to limit the date/time range during which they have access rights. Once a user is registered on the system, you can reset their validity period at any time to allow/disallow access without having to delete and recreate the user each time they need access.

A user's basic access rights are inherited from the User Group to which they are assigned, but you can grant additional access rights on a per-user basis using the **Extra Rights** tab on the **User Details** screen (if you have the appropriate extra memory installed on your controllers).

Adding a permanent user

1. In ACT Manage, click **Add User** on the **Home** screen, or click **Manage > Users**, then click **Add User** in the top right corner of the **Users** screen.

   The **User Details** screen displays.
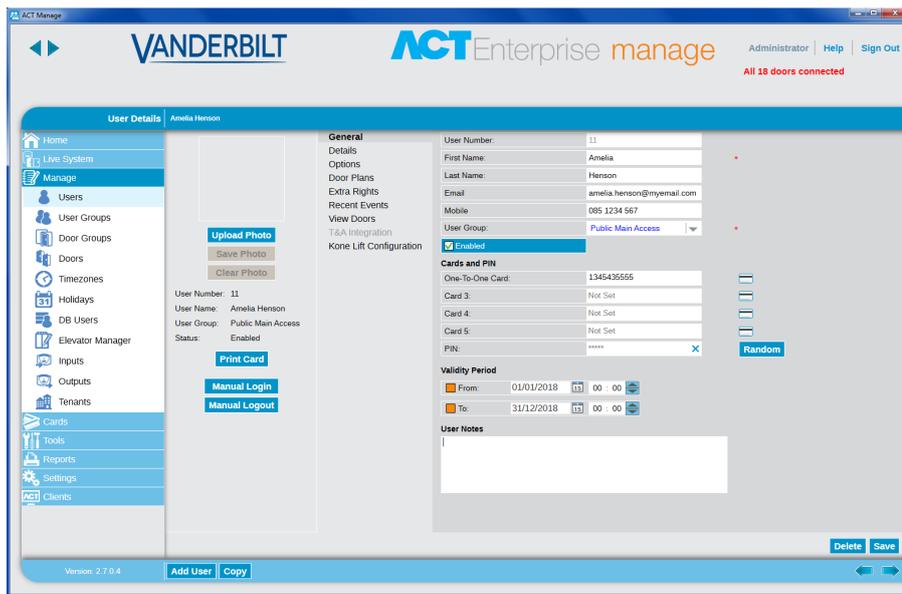
2. On the **User Details** screen, enter information about the new user.

   For more information on the tabs and fields available on this screen, see *The User Details screen* on page 89.

3. Click **Save** to create a record for a permanent user based on the supplied information.

Adding a temporary user

1. In ACT Manage, click **Manage > Users**, then click **Add Visitor** in the top right corner of the **Users** screen.

   The **Visitor Details** screen displays.

2. On the **Visitor Details** screen, enter information about the new temporary user.

   For more information on the tabs and fields available on this screen, see *The Visitor Details screen* on page 94

3. Click the **General** tab, then click **Save** to create a record for a temporary user based on the supplied information.

Copying an existing user

1. In ACT Manage, click **Manage > Users**, then using the **Search**/**Advanced Search** options on the **Users** screen, find and select the existing user you want to base your new user(s) on.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

2. On the **User Details** screen, click **Copy**.

   The **Copy Users** screen displays.
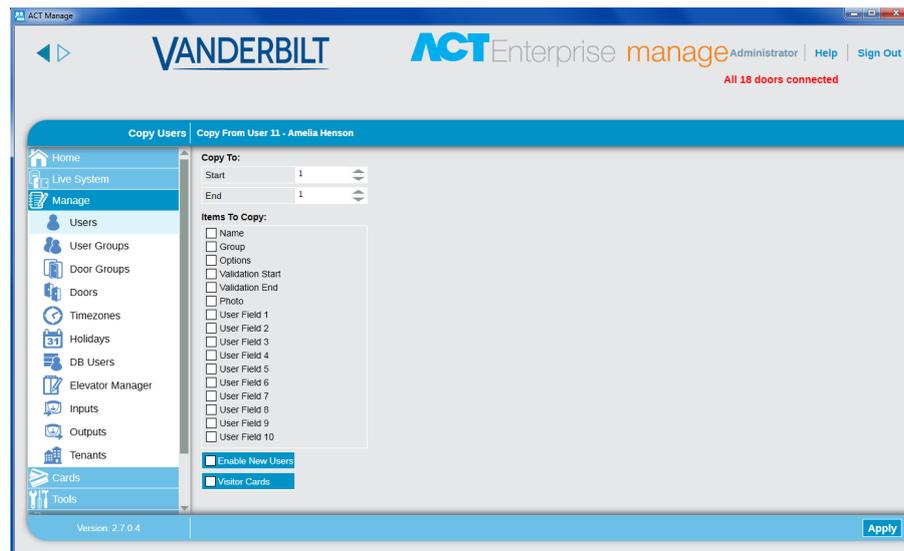
3. Specify the start and end range of users you want to copy selected details to.

   If the users already exist, their current details are overwritten. If they do not already exist, users with the copied details are created.

   You should verify whether or not user IDs in the specified range are already in use before you copy user details.

4. Select the check box for each property from the selected user you wish to copy to the specified existing/new users.

5. To enable any new users created by the operation, select the **Enable New Users** check box.

6. To assign visitor cards for any new users created by the operation, select the **Visitor Cards** check box.

7. Click **Apply**. The selected details are copied to the specified new/existing user records.

   If you created new users, you may want to edit additional properties for them on the **User Details** screen now.

Notes:

- **First Name** and **User Group** are mandatory fields for permanent and temporary users. At a minimum, you must specify values for these before you can save a new user record.

- The user PIN defaults to the PIN of the assigned User Group unless you specify an alternative PIN.

- The **User Number** field is automatically populated with the next available number.

3.3.2 Check which doors a user can access

You can select any user in ACT Manage and view a list of all the doors they have been granted access to.

Checking which doors a user can access

1. In ACT Manage, click **List Users** on the **Home** screen, or click **Manage > Users**, then using the **Search/Advanced Search** options on the **Users** screen, find and select the user whose access rights you want to check.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

2. Click the **View Doors** tab on the **User Details** screen.

3. The panel on the right lists all doors the user has access to, and the time zone during which their

access rights are valid.

Note: Door access is determined in three ways:

1. The user gets access to all doors granted through their user group's access rights.

2. The user can have extra rights assigned.

3. The user can have door plans assigned.

3.3.3 Set access rights for an individual user

In ACT Enterprise, all users must be a member of a user group, and they inherit their basic access rights from that user group.

ACT Manage allows you to assign additional access rights for door groups to a specific user using the **User Details > Extra Rights** tab, or to access rights for individual doors using the **User Details > Door Plans** tab. Each controller must have an additional memory card installed.

The **Extra Rights** tab allows you to assign up to 16 extra door group and time zone combinations to the user. These are only available for controllers with the right capabilities, including extra memory. Please consult your access control installer if you want this option made available. A user can access the set of doors during the period specified by the corresponding time zone.

The **Door Plans** tab allows you to assign specific doors with time zones to a user. These are only available for controllers with the right capabilities, including extra memory. Please consult your access control installer if you want this option made available.

For more information on creating user groups, see *Add a user group* on page 41.

For more information on creating users, see *Add a user* on page 35.

For information on creating time zones, see *Add a time zone* on page 33.

For more information on specifying group access rights, see *Set group access rights* on page 41.

Setting access rights for a door group for an individual user

1. In ACT Manage, click **Manage > Users**, then using the **Search**/**Advanced Search** options on the **Users** screen search for the user for which you want to set access rights.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

2. Click the user's name in the search results area to view details of that user on the **User Details** screen.

3. Click the **Extra Rights** tab on the **User Details** screen.

   The panel at the bottom of the screen shows the door/time zone combinations the user has inherited from their user group.
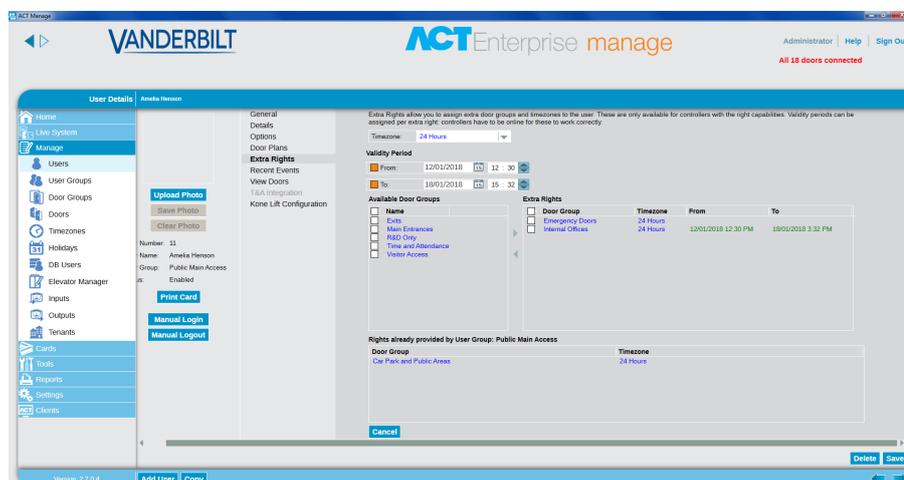
4. Select the **Time Zone** for extra rights you want to assign to the user.

5. (**Optional**) You can limit the time period for which extra rights are valid:

   - To specify a start date for the rights, select the **From** check box and select a start date and time.

   - To specify an end date for the rights, select the **To** check box and select an end date and time.

6. Select a door group from the **Available Door Groups** list and click the right-arrow (▶) to add it to the **Extra Rights** list.

   or

   To add access to all door groups for the selected time zone, click the double-right-arrow (▶▶). If there are more than 16 door groups, you see a warning message and only the first 16 are copied across.

   Note: The right-arrow is disabled (▷) until you have selected both a time zone and a door group. The double-right arrow is disabled (▷▷) until you have selected a time zone.

7. Click **Save** when you have added all required extra rights.

Setting access rights for a door for an individual user

1. In ACT Manage, click **Manage > Users**, then using the **Search**/**Advanced Search** options on the **Users** screen search for the user for which you want to set access rights.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

2. Click the user's name in the search results area to view details of that user on the **User Details** screen.

3. Click the **Door Plans** tab on the **User Details** screen.

   The panel at the bottom of the screen shows the door/time zone combinations the user has inherited from their user group.
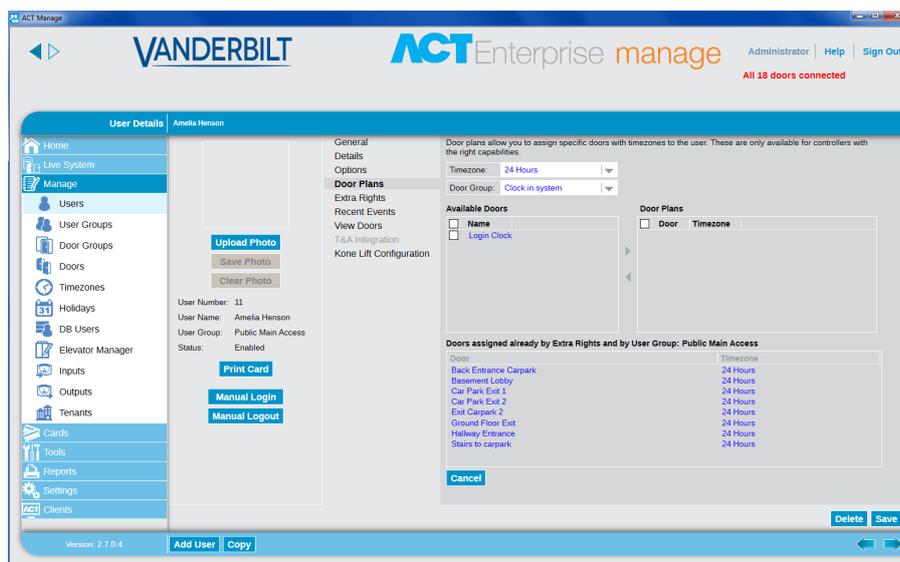
4. Select the **Time Zone** for the door plans you want to assign to the user.

5. Select a door group from the **Door Group** drop-down list.

   The **Available Doors** list shows the doors in the selected door group.

6. Select a door from the **Available Doors** list and click the right-arrow (▶) to add it to the **Door**

Plans list.

or

To add access to all doors for the selected time zone and door group, click the double-right-arrow ( ).

Note: The right-arrow is disabled ( ) until you have selected a time zone, door group and door.

7. Click **Save** when you have added all required door plans.

3.3.4 Extend user validity

You may optionally assign a validity period to users.

- If you do not specify a validity period, the user is always valid.

- If a **From** validity date and time is specified, this is the time from which the user is allowed access. Access is denied to the user before this time.

- If a **To** validity date and time is specified, this is the last time that access is allowed to the user. After this time, access is denied.

- Some controllers also support a validity time, as well as date. If no time is specified, or the controller doesn't support a time, the assumed time is midnight on the specified date.

ACT Manage allows you to:

- Extend the validity of a single user – see *Extending the validity of a single user* below

- Extend the validity of multiple users – see *Extending the validity of multiple users* below

Extending the validity of a single user

1. In ACT Manage, click **Manage > Users**, then using the **Search**/**Advanced Search** options on the **Users** screen search for the user for which you want to extend validity.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

2. Click the user's name in the search results area to view details of that user on the **User Details** screen.

3. At the bottom of the **General** tab, under **Validity Period**, ensure the **To** check box is selected, then enter a new **To** date and time for the user's validity.

4. Click **Save**.

Extending the validity of multiple users

1. In ACT Manage, click **Manage > Users**, then using the **Search**/**Advanced Search** options on the **Users** screen search for the users for which you want to extend validity.

   For more information on the search options on the **Users** screen, see *The Users screen* on page 87.

   or

   In ACT Manage, click **Reports > Validate Users**, then using the **Search**/**Advanced Search** options on the **Validate Users** screen search for the users for which you want to extend validity.

   For more information on the search options on the **Validate Users** screen, see *Validate Users report* on page 130.

2. Select the check box for each user whose validity you want to extend.

3. Click **Set Validity** on the **Users** screen, or **Change Validity Period** on the **Validate Users** screen.

4. Select the **To** check box, then enter a new **To** date and time for the users' validity.

5. Click **Save**.

3.3.5 Add a user group

User groups are used to define common settings and access rights for a set of users.

When you create a user profile, you select one user group to which the user belongs, and their access rights are those assigned to that group. If the group's rights change, then so do those of all members of the group.

If required, users can be assigned additional access rights on the **User Details > Extra Rights** tab or **User Details > Door Plans** tab (see *User Details > Extra Rights Tab* on page 92 or *User Details > Door Plans Tab* on page 91).

ACT Manage allows you to create and edit user groups.

See also:

- *Add a user group through the User Group Details screen* below
- *Add a user group using the User Group Wizard* below

Add a user group through the User Group Details screen

1. In ACT Manage, click **Manage > User Groups**, then click **Add User Group** in the top right corner of the **User Groups** screen.

   The **User Group Details** screen displays.

2. On the **User Group Details** screen, enter information about the new user group.

   For more information on the tabs and fields available on this screen, see *User Group Details Screen* on page 98.

3. Click **Save** to create a record for the user group.

Add a user group using the User Group Wizard

1. In ACT Manage, click **Add User Group** on the **Home** screen to open the **Add User Group Wizard** which walks you through adding a user group step by step.

2. Follow the wizard's onscreen instructions to add a new user group, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

   Note: User groups can optionally be assigned to particular tenancies by selecting one or more sites on the first screen of this wizard. For more information on tenancies, see *Tenancy* on page 121.

3.3.6 Set group access rights

In ACT Enterprise, all users must be a member of a user group, and ACT Manage allows you to set up to eight door group/time zone combinations to specify access rights for all users assigned to a user group.

For more information on creating user groups, see *Add a user group* above.

For more information on creating users, see *Add a user* on page 35.

For information on creating time zones, see *Add a time zone* on page 33.

Setting user group access rights

1. In ACT Manage, click **Manage > User Groups**, then search for the user group for which you want to set access rights.

2. Click the user group's name in the search results area to view details of that group on the **User Group Details** screen.

3. Click the **Access Rights** tab on the **User Group Details** screen.
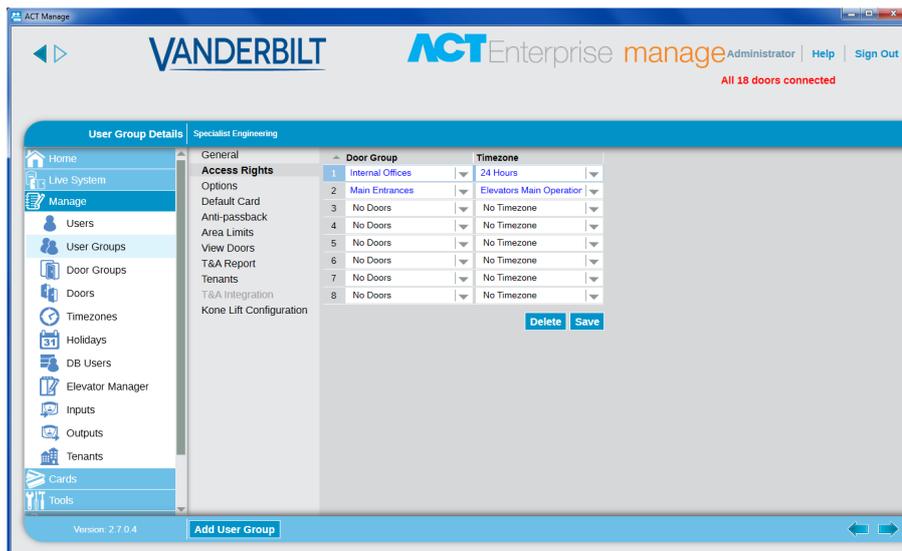
4. Specify up to eight door group/time zone combinations using the drop-down lists provided.

   For each door group/time zone combination, users in the current user group with have access to doors in the selected door group during the period specified by the corresponding time zone.

5. Click **Save** when you have specified all door group/time zone combinations required.

3.3.7 Delete users

There are two types of user in ACT Enterprise, and the deletion of each user type is handled differently:

- A standard user is a person whose access is managed by the ACT software/system. You can configure ACT Enterprise to automatically delete log data associated with a standard user when they are deleted from the system to comply with privacy/GDPR (General Data Protection Regulation) policy in your organisation.

- A DB user is a person using ACT Enterprise software. Audit data related to a DB user is always retained, even if the user is deleted from ACT Enterprise.

Configuring ACT Manage to automatically delete user log data

1. In ACT Manage, click **Settings > General**.

2. From the **Behaviour when deleting users** drop-down list, select what should happen to log data when a user is deleted from ACT Enterprise:

   - **Keep all events for user**

   - **Delete all log events for the user**

3. Click **Save** to save the configured rule to be automatically applied by the system.

Deleting a user from ACT Enterprise

1. In ACT Manage, click **Manage > Users**, then search for the user you want to delete.

2. Click the user name in the search results area to view details of that user on the **User Details** screen.

3. Click **Delete** on the **User Details** screen and confirm the deletion when prompted.

   The user is removed from ACT Enterprise.

   If ACT Manage is configured to delete all events for a user on deletion, the log files are purged of events related to the deleted user.

Deleting a DB user from ACT Enterprise

1. In ACT Manage, click **Manage > DB Users**, then search for the DB user you want to delete.

2. Click the DB user name in the search results area to view details of that DB user on the **DB User Details** screen.

3. Click **Delete** on the **DB User Details** screen and confirm the deletion when prompted.

3.4 Monitoring the system

This section describes how to perform the following system monitoring tasks.

3.4.1 Monitor user activity

ACT Monitor allows you to monitor users' activity.

- In ACT Monitor, on the **Home** screen, the **Recent Events** area includes details of the time, location and summary information for events on the system, including when users access doors, or are denied access. Other events may also be listed, including alarms, system events, controllers and doors going offline, unknown cards, and exit granted/denied. For an event involving a user, such as an **Access Granted** or **Access Denied** event, click the user's name in the **Details** column to view the user's profile on the **User Details** screen. Click the **Back** icon (◀) at the top of the **User Details** screen to return to the **Home** screen.

- In ACT Monitor on the **Users** screen, you can view the last known location of every user on the system. The **Search/Advanced Search** facility allows you to filter for a sub-set of users only. For more information, see *The Users screen* on page 152.
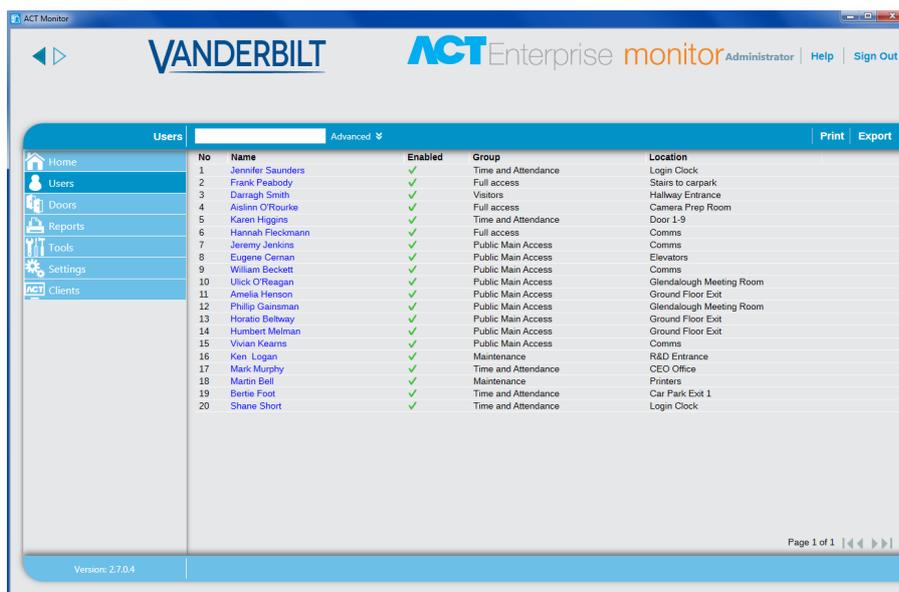
Click the name of any user on this screen to view the **User Details** screen for that user, which includes a summary of their recent events. For more information, see *The User Details screen* on page 153.

- In ACT Manage and ACT Monitor, the **Advanced** search options on the **Reports > Event Analysis** screen allow to you filter for events involving a specific user, or all users in a particular user group. You can further filter for specific event types, events at a particular door or at doors in a particular door group, or events in a specific time frame. For more information, see *Event Analysis Screen* on page 155.

3.4.2 Monitor door activity

ACT Monitor allows you to monitor activity at a number of doors at once, or at a specific door.

- In ACT Monitor, on the **Doors** screen, you can view the last event at every door on the system. The **Search**/**Advanced Search** facility allows you to view the last event for a sub-set of doors only. For more information, see *Doors (ACT Monitor)* on page 154.
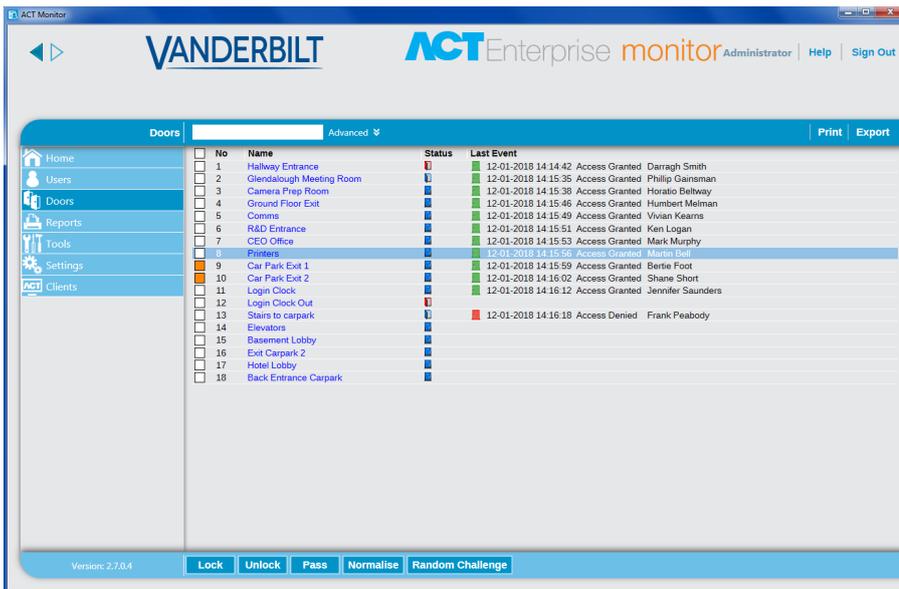
Click the name of any door on this screen to view a report on activity at this door on the **Event Analysis** screen (see *Event Analysis Screen* on page 155).

- In ACT Manage and ACT Monitor, the **Advanced** search options on the **Reports – Event Analysis** screen allow to you filter for events at a specific door, or for all doors in a particular group. You can further filter for specific event types, events for a particular user or users in a particular user group, or events in a specific time frame. For more information, see *Event Analysis Screen* on page 155.
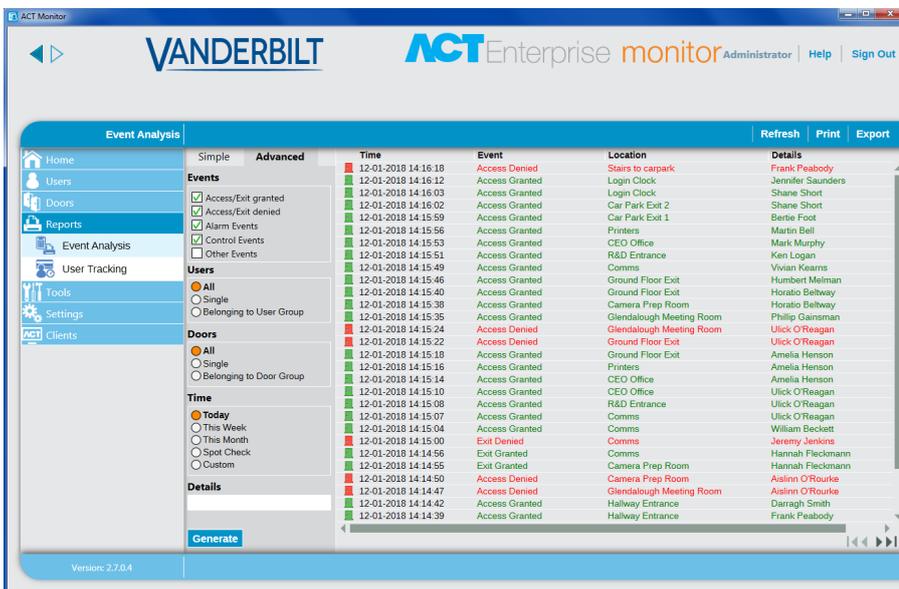
3.4.3 Generate a list of all users on site (Muster Report)

A Muster Report lists all users currently on site. A user is considered to be on site if they entered through a perimeter door, but have not been detected exiting through a perimeter door. If multiple users enter/exit but only one user in the group authenticates at the door, users who did not use their cards may be incorrectly assumed to be present/absent.

Which doors are considered perimeter doors for the site is set in ACT Manage, by selecting the door group containing those doors from the **Perimeter Doors** drop-down list on the **Settings > Doors** tab. For more information, see *Settings > Doors Tab* on page 141.

Notes:

- Muster and absentee reports are only valid if your physical system is configured appropriately. You need access barriers at each entrance and exit to your site, and each user must use their cards when entering/exiting the site.

- Muster reports are generated automatically, without user intervention, if there is a fire event. Configure print/email options for these automatically generated reports in ACT Manage under **Settings > Muster Report**. See *Settings > Muster Report Tab* on page 143.

Generating a muster report

1. In ACT Manage or ACT Monitor, click **Reports > User Tracking**.

2. At **Report**, select **Muster**.

3. At **Time**, select whether you want the report for **Today** or for a **Custom** period.

   If you select a **Custom** period, additional fields appear where you can specify a date/time range.

4. Click **Generate**.

   You can **Print** or **Export** your report using the links at the top right of the **User Tracking** screen.

   For more information on the **Simple**/**Advanced** search options on the **User Tracking** screen, see *User Tracking Screen* on page 156.

3.4.4 Report on time and attendance (T&A)

ACT Enterprise can generate basic T&A reports based on events at entry and exit doors in the system.

You can also integrate ACT Enterprise with a third party T&A system to avail of more advanced functionality.

Track basic T&A data in ACT Enterprise

1. In ACT Manage, under **Manage > User Groups > User Group Details > T&A Report**, configure core and overtime hour conditions for users in this user group:

   - Select the timezones that cover the **Normal Hours** and **Overtime Hours** for users in this user group. For more information on timezones, see *Time zones* on page 110.

     or

   - Specify the maximum number of normal and overtime hours that users in this user group can work each day.

   For more information, see *User Group Details > T&A Report Tab* on page 101.

2. Assign each applicable user to the user group on the **Manage > Users > User Details > General** tab. See *User Details > General Tab* on page 89.

3. Generate a T&A report under **Reports > Time and Attendance**. Report parameters determine the users, doors, and time period covered by the report. For more information on report options and results, see *Time and Attendance report* on page 137.

Integrate with a third party T&A system

1. In ACT Manage, enable and configure integration with a third party T&A system under **Settings > T&A Integration**. See *Settings > T&A Integration Tab* on page 147.

2. To enable T&A integration for all users in a user group, go to **Manage > User Groups > User Group Details > T&A Integration** and select the **Enable T&A Integration** check box. See *User Group Details > T&A Integration Tab* on page 101.

3. To enable/disable T&A integration for an individual user (overriding the default for their user group), go to **Manage > Users > User Details > T&A Integration** and select **Enabled** or **Disabled**.

4. For each tracked user, select the door group with the entry/exit doors that determine their login/logout events for T&A under **Manage > Users > User Details > T&A Integration**.

T&A data are sent by ACT Enterprise to the third party system. Refer to the documentation for the third party system for information on T&A reporting.

3.4.5 Command a door

In ACT Monitor, on the **Home** screen, the **Doors** area shows the status of all doors on the system. Hover over the icon for any door to see its status in a popup. You can command a door by selecting the door, then clicking **Lock**, **Unlock**, **Pass** or **Normalise** at the bottom of the screen.

Note: You must have the right to command doors before you can use these actions.

3.4.6 Add a rule

Rules enable you to automate the ACT Enterprise system to take a specific action in response to trigger events. You can add, edit, and delete rules in ACT Manage.

i	ACT Manage will not prevent you from creating rules with, for example, impossible logic combinations (door is open AND door is closed), or actions that will cause feedback loops (if any emergency exit door is opened, open all emergency exit doors). You should plan and design your rules to avoid such scenarios. Checking the number of **Total Activations** of a rule on the **Rules** screen may provide an indication that a given rule is triggering at an unexpected rate, whether too high or too low.

See also:

- *Rules* on page 107
- *The Rules screen* on page 108
- *The Rule Details screen* on page 108

Add a rule

1. In ACT Manage, click **Manage > Rules**.

2. Click **Add Rule**.

3. Enter a name for the new rule in the **Rule Name** field.

4. Add rule elements (analysers, logic operations, and actions) in the main screen area and connect them as appropriate:

   To add an analyser:

   a. Right-click in the main page, click **New Analyser** in the context menu, then click the required analyser type in the sub-menu. See *Analyser types* on page 108 for information on supported analyser types.

   b. Configure the analyser with the condition that should trigger this rule.

To combine analysers, or to trigger the rule if an analyser evaluates as FALSE, add a logic operation:

    a. Right-click in the main page, click **New Logic** in the context menu, then click the required logic type in the sub-menu. See *Logic operations* on page 110 for information on supported logic operations.

    b. Select a logic operation from the drop-down list.

    c. Connect each analyser to be evaluated or combined to the logic operator. To do this, drag the black circle from the top-right of an analyser to the logic box.

Add an action:

    a. Right-click in the main page, click **New Action** in the context menu, then click the required action type in the sub-menu. See *Action types* on page 109 for information on supported action types.

    b. Select an action from the drop-down list.

    a. Connect each analyser (or logic operation) to the action triggered when the analyser (or logic operation) evaluates as TRUE. To do this, drag the black circle from the top-right of an analyser (or logic) box to an action box.

    Note: You can add multiple actions to a rule.

5. Click **Save**.

4 ACT ServerClient Reference

This section describes the following:

See also:

- *Navigating ACT Enterprise client interfaces* on page 11

4.1 About ACT ServerClient

ACT ServerClient offers a range of tools for managing the ACT Enterprise database and server. Using this application, you can stop/start the service, assign a new database, upgrade controller firmware, monitor controller communications in great detail, and perform a range of other specialised tasks. Events can be purged, users exported or imported, and simple backups can be done.

4.2 Live System (ACT ServerClient)

This screen displays information about the live ACT Enterprise system.

- **Service** – This area shows information about the ACT Enterprise Windows service. You can check service details and state, and stop and start the service from here. This Windows service must be running in order to use ACT Enterprise. The service normally starts up automatically when the server machine reboots. You can **Stop** and **Start** the service in those exceptional cases where you need to reboot the service. (You can also use the **Restart** option, which stops then starts the service.) When you stop the service, all activity on clients ceases abruptly and all controllers are disconnected from the software, so you should warn operators before stopping and restarting the service. To check which operators are currently active on the system, use the **DB Users** screen (see *DB Users* on page 51).

- **Server** – This area shows information about the ACT Enterprise server: whether it is currently running, and whether the database is connected. The server may be down if either the Windows hosting service has not started, or if it cannot contact a valid ACT Enterprise database. If the service port has been changed from the default in your organisation, you may need to enter the new **Service Port** and click **Reconnect** to access the server. For more information, see *Change the default service port* on page 25.

  If there is a problem with your installation, Vanderbilt support may request that you click **Diagnostics** to generate a text file with basic information on your environment, product version, and infrastructure. They may also request that you switch between **Default Tracing**/**Verbose Tracing** and pass on log files that can be used to diagnose system problems.

- **Controllers** – This area shows a list of registered and enabled controllers (and disabled controllers

with enabled doors) and their current states. You can click the expand icon ( ) beside a controller name to view a list of doors connected to that controller and their current states.

- **Recent Events** – This area shows the time, location, event type and details for recent events (live).

4.3 Database

This screen displays information about the ACT Enterprise database.

- **Database Settings** – This area shows details of the current ACT Enterprise database, including name, status and a summary of the data types and volumes. You can change which database is in use, or create a new database from here. You can also specify a connection string. If you have a legacy ACT Enterprise database, click **Migrate Data** to open a migration tool that can convert that database to the latest SQL Compact or SQL Server format. See *Migrate a database* on page 24 for more information.

- **Tools** – This area enables you to export and import user details, and to purge log events.

    - **Export Users** – This tool enables you to export the current set of users to a CSV (comma separated value) file. All enabled users are exported. This list of users can be later restored using the **Import Users** tool.

    - **Import Users** – This tool enables you to restore a set of users previously exported, or to import a new set of users. You can choose to delete the existing set of users in the database or to attempt to merge the new list with the existing users. Where an imported user has the same user number as an existing user, the imported user overwrites the existing user.

    - **Export or Import Photos** – To export all user photos from ACT Enterprise, click **Export or Import Photos**, click **Yes**, then select a folder and click **OK**. Photos are exported in JPG format with the following file naming convention: **User<user number> <Last Name>-<First Name>**.

      To import user photos, click **Export or Import Photos**, click **No**, then select a folder and click **OK**. Photos must be in JPG, GIF, BMP, PNG or TIFF format, and have the following file naming convention: **User<user number> <Last Name>-<First Name>**. ACT Enterprise resizes images and converts files to JPG format during import.

    - **Purge Log Events** – When the log events table grows large, it has a detrimental impact on system performance. It is highly recommended that you regularly purge the log events table of unwanted, legacy events. You can choose to purge all events, all but events in the last one month, all but events in the last three months, or all but events in the last six months. Purging log events can take a considerable amount of time.

      Note: You can also configure ACT Enterprise an automatic purge schedule in ACT Manage under **Settings > Schedule Log Event Purge**. For more information, see *Settings > Schedule Log Event Purge Tab* on page 145.

4.4 Backups

This screen enables you to schedule automatic backups of the ACT Enterprise database, to create a database backup immediately, or to restore the system from a database backup.

The database management functions on this screen are primarily intended for use with SQL Compact databases (.SDF files), and this documentation describes how the database backup and restore functions work with respect to a SQL Compact database specifically.

If you are using SQL Server, Vanderbilt recommend that you use the more powerful database admin tools available in SQL Server to implement your backup policy.

- **Backup Options** – This area enables you to configure automated daily database backups.

  To define a backup schedule, select the **Automatic Backups On?** check box, then select the time of day that backups should be performed from the **Daily Auto Backup Time** drop-down (this should be a time that you expect minimal system usage), select the number of backups that should be retained from the **Backup Rolls Over Days** drop-down, then click **Save**. Click **View Backups** to the right of this area to open the default folder containing ACT Enterprise database backups.

  By default, automated database backups are saved to a sub-folder of where ACT Enterprise is installed, for example, C:\ProgramData\Access Control Technology\ACT Enterprise\Backups. To specify a custom location for automated backups, click **Custom Backup Folder**, browse to and select the required folder, click **OK**, then click **Save**. Click **View Backups** to the right of this area to open the custom folder containing automated database backups. To stop using a custom location for automated backups, click **Clear**, then **Save**.

- **Manual Backups and Restores** – This area enables you to manually backup or restore an ACT Enterprise database.

  By default, manual database backups are saved to a sub-folder of where ACT Enterprise is installed, for example, C:\ProgramData\Access Control Technology\ACT Enterprise\Backups. To specify a custom location for manual backups, click **Custom Folder**, browse to and select the required folder, then click **OK**. To stop using a custom location for automated backups, click **Clear** and confirm when prompted.

  Click **View Backups** to the right of this area to open the folder containing manual database backups.

  Click **Manual Backup** to backup the ACT Enterprise database .

  Click **Restore** to select a backup database from which to restore the system, then confirm the restore operation when prompted.

  > **i** If you restore the system from a backup database, you will lose any changes or additions to the system implemented since the backup was created.

4.5 Upload

This screen allows you to upload system information from one or more connected controllers.

> ⚠ This functionality is intended to be used for emergency disaster recovery only, where the ACT Enterprise database has been lost or corrupted irretrievably. Data you upload from a controller will overwrite existing data in your database. If you attempt to upload configuration information from multiple controllers, ACT Enterprise will attempt to identify the controller with the most complete dataset and upload from that controller only to limit potential duplication or overwrites.
>
> Controllers store a limited subset of the configuration information for your system, for example connected doors (but not door groups), card numbers and access rights. You must manually complete system re-configuration following an upload of settings from controllers to add missing information, for example, door groups.
>
> If you upload card details from a controller, the name associated with the card is only stored if the **Settings > Controller Settings > Download Names** option was selected in ACT Install when the controller settings were last saved.

To upload data from one or more controllers to partially restore your system, ensure that the controllers are online and accessible, then:

1. Add controller details to your system using ACT Install (see *Add a controller* on page 15).

   or

   Select the **Choose new controller** check-box on the **Upload** screen, enter the controller connection details, and click **Add Upload Controller** to add connection details for that controller to your system

2. Select the check box for each controller from which you want to upload data on the **Upload** screen, then click **Start Upload**.

4.6 DB Users

This screen displays information about the ACT Enterprise operators (database users).

- **DB Users Currently Online** – Displays a list of operators currently online. The particular ACT Enterprise application in use is shown (for example, ACT Manage), plus information on when the operator's logon started, activity duration, PC location and state.

  You can log an operator out by selecting the check box to the left of their name and clicking **Disconnect**. This action cancels any activity the operator is currently performing, abruptly.

- **User's Recent Actions** – Displays information on recent activities performed by the selected operator.

4.7 Firmware Upgrade

Updating firmware to the latest available version from the manufacturer is highly recommended.

When you update the firmware on a controller, it shuts down normal operation for the period of the upgrade, which can take several minutes depending on the network conditions. All data about users, cards, and access rights are deleted from a controller when the firmware is updated.

You can optionally unlock doors connected to a controller while the firmware upgrade is in progress to allow users to gain access. If you do not want to leave connected doors unlocked for the duration of the upgrade, only update firmware when you are confident that the controller is not required.

If a firmware upgrade file is available, this screen allows you to select the firmware and which controllers to upgrade. You must have the password required to access the firmware upgrade in order to apply it.

1. Click **Select Firmware** to open a dialog where you can browse to and select the firmware file you are upgrading to.

   Ensure that you have a firmware version later than the version currently on your controller types.

2. In the **Password** field, enter the firmware password (obtainable from Vanderbilt). This is validated when you click **Upgrade Firmware**.

3. Optionally, you can choose the **Controller Type** to filter the controller list at the bottom of the screen for controllers matching that type.

4. From the controller list at the bottom of the screen, select each controller for which you want to upgrade firmware.

   Note: Controllers must be online in order for you to do an upgrade, but all controllers are listed.

5. To open doors connected to the selected controllers, allowing free access, while the firmware upgrade is in progress, select the **Open doors during upgrade?** check box. If doors are not opened, users cannot gain access until the upgrade is complete and data synced to the controller.

6. To automatically sync data to the selected controllers following the firmware upgrade, select the **Do full download when finished flash upgrade?** check box.

If you do not select this option, you must manually sync data to the controllers using the System Synchronise tool in ACT Manage or ACT Install (see *Synchronise controller information* on page 30) following the firmware upgrade.

7. When you are ready, click **Upgrade Firmware**.

If the password is correct, the controller types match the firmware type, and if they are all online, then the firmware is upgraded.

4.8 Monitoring

This screen allows you to select one or more controllers to monitor their communications with the software. This feature can be useful for in-depth trouble-shooting.

- **Controllers** – Displays a list of controllers on the system. You can select particular controllers to monitor/stop monitoring, and specify the number of minutes for which monitoring should last. Results of a trace of the activity between the controller(s) and the software is shown in the **Communications** area.

  If you want to view details from an existing log file, you can select it here too.

- **Communications** – This area shows all communications between controllers and ACT Enterprise. You can clear this area by clicking **Clear View**. Details are also saved into the ServerClient.log log file, available through the **View Files** button. This log file can be sent to Vanderbilt for analysis.

4.9 Register Software

This screen allows you to manage and register serial keys for ACT Enterprise.

- To add a new key, click **Add Key**, enter a valid serial key in the popup that displays, and click **Add**.

- To delete an existing key, select the key in the **Serial Key** list, click **Delete Key**, and confirm the deletion when prompted.

- To register a key, select the key in the **Serial Key** list, and click **Register**.

i	- If you have multiple registration keys, you must register each one separately. - The serial key for ACT Enterprise Lite is auto-registered.

5 ACT Install Reference

This section describes the following:

See also:

5.1 About ACT Install

ACT Install manages the access control hardware on the system. It is used to add or update controllers, doors and I/O modules.

5.2 Live System (ACT Install)

This screen provides an overview of the live system.

The system tree on the left hand side of the screen allows you to view all configured controllers and their connected doors, as well as I/O modules on the network. The icon for each entity indicates its status. Hover your mouse over an icon to see a popup describing the status. Right-click a controller or door in the tree structure to see a context menu with the following options:

- **Expand All** – Select to fully expand the tree structure, showing all doors connected to all controllers.

  Note: You can expand the list of doors for a particular door by clicking the ▶ icon to the left of the controller name.

- **Collapse All** – Select to collapse the tree structure, showing all controllers, but no connected doors.

  Note: You can collapse the list of doors for a particular door by clicking the ▾ icon to the left of the controller name.

- **Actions** – Select to view a list of actions you can perform on a door: **Lock**, **Unlock**, **Pass**, **Normalize**, **Switch Outputs ON**, **Switch Outputs OFF**.

- **Validate** – Select to validate a door, confirming whether it is connected and responding to commands. For more information, see *Validation Wizard* on page 79.

- **Details** – Select to view more information on the selected controller/door. For more information, see *Controller Details* on page 56 or *Door Details Screen* on page 65.

The **View Options** drop-down menu at the top right of the screen also allows you to filter what information is displayed in the tree structure.

- To view one or more of **Controllers**, **Doors** and **I/O Modules**, select the appropriate boxes under **View Options > View**.

- To view only those doors reporting problems, click **View Options > View > Problem Hardware**. Examples of possible problems are tampering detected, low battery, or the glass on a Break Glass Monitor broken.

  Note: You cannot view **Problem Hardware** at the same time as controllers, doors or I/O modules.

Other links at the top right of the screen provide quick access to the QuickSetup wizards for adding controllers and doors, and for auto-discovering entities on the network.

The panel on the right-hand side of the screen shows live information on events occurring across the system. For each event, the time, location, event type and details are shown.

Click the **Pause** button at the bottom of the screen to pause the stream of events being displayed. This allows you to examine the details of one or more events currently on screen without them scrolling out of view.

Quick setup buttons at the top of the screen provide easy access to the **Add Controller**, **Add Door** and **Autodiscover** wizards.

See also:

- *Add Controller* below

- *Add Door* below

- *Autodiscovering* on the facing page

5.3 Quick Setup

The **Quick Setup** menu contains links to a number of wizards which take you through the setup of common components step by step.

The following sections describe the wizards available in this menu:

5.3.1 Add Controller

Follow the wizard's onscreen instructions to add and configure a new controller, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

You can edit the controller settings later through the **Controller Details** screen (see *Controller Details* on page 56).

5.3.2 Add Door

Follow the wizard's onscreen instructions to add and configure a new door, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

You can edit the controller settings later through the **Door Details** screen (see *Door Details Screen* on page 65).

5.3.3 Add Elevator

Follow the wizard's onscreen instructions to add and configure a new elevator, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end.

- **Step 1: Select I/O Modules.** Select which I/O modules are connected to the elevator.

- **Step 2: Set Floors.** Select which outputs are connected to elevator floors.

- **Step 3: Finish.** The results of the add elevator operation are shown: the number of floors added/removed and their current statuses.

5.3.4 Autodiscovering

Follow the wizard's onscreen instructions to add and configure controllers and their related doors, clicking **Next** in the bottom right of the screen after each step and **Finish** at the end. For more information, see *Auto-discover networked controllers* on page 19.

Note: Older ACT controllers cannot be autodiscovered (for example, ACT1000, ACT2000 and ACT3000).

You can edit the controller and settings later through the **Controller Details** screen (see *Controller Details* on the next page) and the **Door Details** screen (see *Door Details Screen* on page 65).

5.4 Advanced Setup

Advanced Setup allows you to configure new controllers and doors without using the Wizards provided. You can also edit existing controllers and doors. More settings are available through the **Advanced Setup** screens than through the Wizard.

You can also add and configure I/O modules, DVRs, cameras and card settings.

The following sections describe the functions available in this menu:

5.4.1 Controllers/Hub Groups

A controller is a device which stores card details and provides managed access for one or more doors. ACT Install allows you to configure controller properties, and to specify which doors are connected to that controller.

This section describe the screens and tabs accessed through this menu.

5.4.1.1 Controllers

The following table describes the search fields and results columns on the **Controllers** screen.

Field Name	Description
Search	Enter all or part of the name of the controller you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area.
Advanced	Click **Advanced** to search for a controller by number and/or name. If you specify a **Controller Number**, an exact match is returned. If you specify a **Controller Name**, partial matches are returned.
No	The unique number that identifies this controller on the system. (Sortable.)
Controller Name	The controller's name. Click to view full details for this controller on the **Controller Details** screen (see *Controller Details* below). (Sortable.)
Controller Type	The controller type.
Firmware	The firmware version on the controller (where available).
Comms	The IP address or NetBios name of the controller.
MAC Address	The MAC address of the controller.
Status	The controller status. Hover your mouse over the icon to see the status in a popup.
Doors	The number of doors connected to the controller. Click to view a list of the connected doors on the **Doors** screen (see *Doors Screen* on page 64).
I/Os	The number of I/O modules connected to the controller. Click to view a list of the connected I/O modules on the **I/O Modules** screen (see *I/O Modules Screen* on page 70).
Memory Card	A green check-mark is displayed for controllers that support a memory card. A controller with a memory card can support extra cards, rights, and door plans. These additional capabilities are reported on the **Capabilities** tab.
Enabled	A green check-mark is displayed for controllers that are enabled.

5.4.1.2 Controller Details

The **Controller Details** screen has a number of tabs showing different settings for the selected controller. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Controller Details > General Tab* on the facing page.
- **Communications** tab. For more information, see *Controller Details > Communications Tab* on the facing page.
- **Doors** tab. For more information, see *Controller Details > Doors Tab* on the facing page.
- **I/O Modules** tab. For more information, see *Controller Details > I/O Modules Tab* on page 58.
- **Output Options** tab. For more information, see *Controller Details > Output Options Tab* on page 58.
- **Operations** tab. For more information, see *Controller Details > Operations Tab* on page 59.
- **Capabilities** tab. For more information, see *Controller Details > Capabilities Tab* on page 60.
- **Cluster** tab. For more information, see *Controller Details > Cluster Tab* on page 60.
- **Firmware** tab. For more information, see *Controller Details > Firmware Tab* on page 60.

5.4.1.3 Controller Details > General Tab

The following table describes the data that appears on the **Controller Details > General** tab.

Field Name	Description
Controller Name	The controller name.
Controller Number	The controller number. This cannot be edited once the controller is first saved.
Controller Type	The controller type.
Enabled	If this check box is selected, the controller is enabled on the system; if not, it is disabled.

5.4.1.4 Controller Details > Communications Tab

The following table describes the data that appears on the **Controller Details > Communications** tab.

Field Name	Description
Communications Master	Whether the ACT Enterprise server communicates directly with the controller, or communicates via another controller (hubbed). If hubbed via an intermediate controller, that controller should be selected here. If a hubbed controller is not identified in this way, its details cannot be saved.
Connection Type	If you are communicating directly with the controller, the connection type is shown. • TCP/IP – Select if communicating over TCP/IP. • RS232 – Select if connecting directly to a single controller using a simple RS232 serial lead. The maximum distance for direct connection is 30m.
IP Address Port	The IP address or NetBios name and listening port of the ACT LAN Interface device. Port number should always be 10001. This field only appears if **Direct to ACT Enterprise** is selected at **Communications Master** and **TCP/IP** is selected at **Connection Type**.
COM Port Speed	The serial communications port to which the access control system is connected and the supported communication speed.
Encryption Key	An Encryption key consisting of a 10-digit number may be specified to prevent unauthorized access to the controllers. Ensure this Encryption key matches the Password programmed into the controllers. Encryption is available only for modem or TCP/IP locations.
World Time Zone	The world time zone the controller is operating in.
Web Page	If the controller has an on-board web interface, the URL is shown here.

Click **Test Connection** to check that there is a live connection between the database and the controller.

5.4.1.5 Controller Details > Doors Tab

The following table describes the data that appears on the **Controller Details > Doors** tab.

Field Name	Description
Address	The address of the door on the controller.

Field Name	Description
Name	The door name.
Enable	If this box is selected, the door is enabled.
In DB	If this box is selected, the door details are recorded in the database. De-selecting this box deletes the door from the database when you click **Save**.

5.4.1.6 Controller Details > I/O Modules Tab

The following table describes the data that appears on the **Controller Details > I/O Modules** tab.

Field Name	Description
Address	The address of the I/O module on the controller.
Name	The I/O module's name.
Enable	If this box is selected, the I/O module is enabled.
In DB	If this box is selected, the I/O module's details are recorded in the database. De-selecting this box deletes the I/O module from the database.

5.4.1.7 Controller Details > Output Options Tab

Controller output options allow the onboard OP2, OP3 and AUX outputs on a multi-door controller to perform different functions to those normally programmed by the door or user settings.

The following table describes the data that appears on the **Controller Details > Output Options** tab.

Field Name	Description
Outputs (Door 1)	
AUX for all doors	When this option is selected, the AUX output on door 1 operates if the AUX output for any of the doors connected to the controller is active.
OP2 = Tech Fault	When this option is selected, the AUX output on door 1 operates if a technical fault condition exists. Technical faults include mains faults, tampers or doors offline.
OP3 = Any Door Open	When this option is selected, the OP3 output on door 1 operates if any of the doors connected to the controller are open.
Outputs (Door 2)	
AUX = Users present	When this option is selected, the AUX output on door 2 operates while one or more users are within the anti-passback or perimeter area (if configured). The output activates immediately when a user enters the defined area, and de-activates when all users have exited. The deactivation of the output is postponed by the period of time defined by the delay timer. This may be used (for example) to switch off lighting when no users are present, or to indicate to an alarm system that it is clear to arm.
OP2 = User Limit A	When this option is selected, the OP2 output on door 2 operates when the number of users within the anti-passback or perimeter area reaches or exceeds **User Limit A** specified on the **Settings > Doors** tab (see *Settings > Doors Tab* on page 141).
OP3 = User Limit B	When this option is selected, the OP3 output on door 2 operates when the number of users within the anti-passback or perimeter area reaches or exceeds **User Limit B** specified on the **Settings > Doors** tab (see *Settings > Doors Tab* on page 141).

5.4.1.8 Controller Details > Operations Tab

The options available on this tab depend on the controller type.

The following table describes the options that appear on the **Controller Details > Operations** tab.

Field Name	Description
General	
Web Server	This field appears if the controller has an on-board web interface for configuration and viewing diagnostics. If your controller has an on-board web interface, the URL is shown on the **Controller Details > Communications** tab (see *Controller Details > Communications Tab* on page 57).
	If you manage this controller through ACT Enterprise instead of through the on-board web interface, de-select this check box.
Support OSDP	If selected, this controller supports readers that use OSDP (Open Supervised Device Protocol). The controller hardware must also be configured to support OSDP. Refer to the controller installation guide for more information.
	Note: OSDP readers are only supported on door 1 of an ACT1500-family controller. OSDP readers do not work on controllers without the OSDP jumper. For more information on configuring an OSDP reader, see *Door Details > OSDP Readers Tab* on page 65.
Auto Daylight Savings	If selected, the controller automatically adjusts for daylight savings.
Keypad sound	If selected, the controller makes a small audible beep for confirmation whenever a key is pressed.
Show status	If selected, the controller shows the current status of each door on its LCD display. Normally when all doors are closed, the display shows only the current date and time. When the status of a door changes, it is shown periodically on the display until it reverts to normal.
Show events	If selected, the controller shows all events on its LCD display as they occur. The event is displayed for 2 seconds or until superseded by another event.
Attendance terminal	If selected, the controller logs entrance and exit events for time and attendance purposes. Marking a controller as an attendance terminal means Clockin and Clockout events are generated on door 1, instead of access granted events. An attendance terminal should only be assigned if door 1 is acting as a Time & Attendance recorder.
Tech fault bleeps	If selected, the controller bleeps periodically if a technical fault occurs. Example technical faults: mains faults, tampers and doors offline.
User limiting	If selected, when the number of users inside the perimeter area is equal to the maximum of either User Limit A or User Limit B then the controller prevents any more users from entering. For more information, see *Settings > Doors Tab* on page 141.
Printer	
This section appears if the controller supports printing to a local printer. See the controller installation guide for information on how to connect and configure a local printer.	
Log to local printer	Select this check box to print log events from this controller to the local printer.
Printer handshake	Select this check box if the local printer requires a handshake before printing.

5.4.1.9 Controller Details > Capabilities Tab

This screen shows the hardware capabilities of the controller. For example, the number of doors it can control, the number of users it can support, and the number of I/O modules.

5.4.1.10 Controller Details > Cluster Tab

If this controller is the cluster master, select the **Cluster Master** check box.

If another controller is the cluster master, select it from the **Cluster Master Controller** drop-down list.

Controllers connected to the cluster master pass information about users entering and exiting, and the cluster master relays that information to others in the cluster. This information is used to prevent a user entering through multiple doors in the cluster where anti-passback is enabled.

5.4.1.11 Controller Details > Firmware Tab

This screen shows the version of firmware currently installed on the controller.

5.4.2 Hub Groups

A hub group acts as a virtual controller for the management of a group of eLock hubs. Up to 4 eLock hubs can be connected to a single hub group to share the management of a set of up to 32 wireless locks. When an eLock connects wirelessly to any eLock hub, that hub shares the information from that eLock with other eLock hubs in the hub group.

ACT Install allows you to add hub groups to the system and to configure properties for their operation.

This section describe the screens and tabs accessed through this menu.

5.4.2.1 The Hub Groups screen

The following table describes the columns on the **Hub Groups** screen.

Field Name	Description
Hub Group Name	The hub group name. Click to view full details for this hub group on the **Hub Group Details** screen (see *The Hub Group Details screen* below). (Sortable.)
Hub Group	The unique number that identifies this hub group on the system. (Sortable.)
Controllers	The number of controllers connected to this hub group. Click to view full details for this hub group on the **Hub Group Details** screen (see *The Hub Group Details screen* below). (Sortable.)
Doors	The number of doors connected to the hub group. Click to view a list of the connected doors on the **Doors** screen (see *Doors Screen* on page 64).

5.4.2.2 The Hub Group Details screen

The **Hub Group Details** screen has a number of tabs showing different settings for the selected hub group. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Hub Group Details > General Tab* on the facing page.
- **eLock Hubs** tab. For more information, see *Hub Group Details > eLock Hubs Tab* on the facing page.
- **eLock Doors** tab. For more information, see *Hub Group Details > eLock Doors Tab* on the facing page.
- **Operations** tab. For more information, see *Hub Group Details > Operations Tab* on page 62.
- **GPI and GPO** tab. For more information, see *Hub Group Details > GPI and GPO Tab* on page 62.
- **Capabilities** tab. For more information, see *Hub Group Details > Capabilities Tab* on page 62.

5.4.2.3 Hub Group Details > General Tab

The following table describes the data that appears on the **Hub Group Details > General** tab.

Field Name	Description
Hub Group Name	The hub group name.
Hub Group	The hub group number. This cannot be edited once the controller is first saved.

5.4.2.4 Hub Group Details > eLock Hubs Tab

The following table describes the data that appears for each eLock hub listed on the **Hub Group Details > eLock Hubs** tab.

Field Name	Description
Name	The eLock hub name.
IP address	The IP address of the eLock hub.
Port	The listening port of the eLock hub.
Enable	Select this check box to enable the eLock hub.
In DB	Select this check box to add this eLock hub to the ACT Enterprise database. **Note:** You can only edit details for an eLock hub if the **In DB** check box is selected for that eLock hub.
Details	Click **Details** to view full details for this eLock hub on the **Hub Details** screen (see *Hub Details Screen* on page 63).
Test Connection	Click to test the connection to the eLock hub. If the connection is successful, a green check mark appears beside the **Test Connection** button. If the connection fails, a red cross appears beside the **Test Connection** button.
World Time Zone	Select the time zone for the eLock hubs in this hub group.

5.4.2.5 Hub Group Details > eLock Doors Tab

The following table describes the data that appears for each eLock door listed on the **Hub Group Details > eLock Doors** tab.

Field Name	Description
Address	The local address for the eLock door.
Name	The eLock door name.
MAC address	The MAC address of the eLock door.
Enable	Select this check box to enable the eLock door.
In DB	Select this check box to add this eLock door to the ACT Enterprise database. **Note:** You can only edit details for an eLock door if the **In DB** check box is selected for that eLock door.

5.4.2.6 Hub Group Details > Operations Tab

The following table describes the data that appears on the **Hub Group Details > Operations** tab.

Field Name	Description
General	
Web Server	This field appears if the eLock hubs in this hub group have an on-board web interface for configuration and viewing diagnostics. If your eLock hub has an on-board web interface, the URL is shown on the **Hub Details > Communications** tab (see *Hub Details > Communications Tab* on page 64). If you manage eLock hubs through ACT Enterprise instead of through the on-board web interface, de-select this check box.
Auto Daylight Savings	If selected, eLock hubs in the hub group automatically adjust for daylight savings.
Tech fault bleeps	If selected, eLock hubs in the hub group bleep periodically if a technical fault occurs. Example technical faults: mains faults, tampers and doors offline.
Tamper	If selected, eLock hubs in the hub group log tampers.
Mains fault	If selected, eLock hubs in the hub group log mains faults.

5.4.2.7 Hub Group Details > GPI and GPO Tab

GPI (general purpose input) and GPO (general purpose output) settings are configured for a hub group, and are applied to every eLock hub in the hub group. If you want to use this functionality, contact Vanderbilt for more information on configuring hardware and software support.

5.4.2.8 Hub Group Details > Capabilities Tab

This screen shows the hardware capabilities of the hub group. For example, the number of doors it can control, the number of users it can support, and the number of I/O modules.

5.4.3 eLock Hubs

An eLock hub is a controller that communicates wirelessly with eLocks. Up to four eLock hubs can be gathered into a hub group to manage a common set of doors

You can add eLock hubs to ACT Enterprise from the ACT Install **Hub Group Details > eLock Hubs** tab. Once an eLock hub is added to ACT Enterprise, it appears in the list on the **eLock Hubs** page.

ACT Install allows you to view details of any configured eLock hub, to rename the hub, and to configure communications details for the hub.

This section describe the screens and tabs accessed through this menu.

5.4.3.1 eLock Hubs Screen

The **eLock Hubs** screen lists the eLock hubs configured on the system. eLock hubs are added and configured from the **Hub Group Details > eLock Hubs** screen (see *Hub Group Details > eLock Hubs Tab* on the previous page).

The following table describes the columns on the **eLock Hubs** screen.

Field Name	Description
Hub Group	The hub group number. Click to view full details for this hub group on the **Hub Group Details** screen (see *The Hub Group Details screen* on page 60). (Sortable.)

Field Name	Description
Local ID	The local address for the hub at the controller. (Sortable.)
Name	The eLock hub name. Click to view full details for this eLock hub on the **eLock Hub Details** screen (see *Hub Details Screen* below). (Sortable.)
NetBIOS Name	The NetBIOS name of the eLock hub, if the eLock hub is configured to use DHCP. See *Hub Details > Communications Tab* on the next page for more information. (Sortable.)
IP address	The IP address of the eLock hub, if the eLock hub is configured to use a static IP address. See *Hub Details > Communications Tab* on the next page for more information. (Sortable.)
Port	The listening port of the eLock hub. (Sortable.)
DHCP	Whether the eLock hub is configured to support DHCP. The eLock hub uses DHCP if the NetBIOS name from the sticker on the eLock hub is entered as its IP address on the **Hub Details > Communications** tab. See *Hub Details > Communications Tab* on the next page for more information.
MAC address	The wired MAC address of the eLock hub. This is read from the firmware when ACT Enterprise connects to the eLock hub. (Sortable.)
Status	The eLock hub status. (Sortable.) Options are: - Online - Offline - Disabled
RF MAC address	The wireless MAC address of the eLock hub. This is read from the firmware when ACT Enterprise connects to the eLock hub. (Sortable.)
Firmware	The firmware version on the eLock hub. (Sortable.)
Hardware	The hardware version. (Sortable.)
Enabled	Whether the eLock hub is enabled.

5.4.3.2 Hub Details Screen

The **Hub Details** screen has a number of tabs showing different settings for the selected eLock hub. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Hub Details > General Tab* below.
- **Communications** tab. For more information, see *Hub Details > Communications Tab* on the next page.
- **Capabilities** tab. For more information, see *Hub Details > Capabilities Tab* on the next page.
- **Firmware** tab. For more information, see *Hub Details > Firmware Tab* on the next page.

5.4.3.3 Hub Details > General Tab

The following table describes the data that appears on the **Hub Details > General** tab.

Field Name	Description
Hub Group	The number of the hub group to which this eLock hub belongs.

Field Name	Description
Hub Group Name	The name of the hub group to which this eLock hub belongs.
Local Address	The local address for the hub at the controller.
Hub Name	The hub name. This field is editable.
Hub Type	The hub type.
RF MAC address	The wireless MAC address of the hub. This is read from the firmware when ACT Enterprise connects to the eLock hub.
Enabled	If this check box is selected, the eLock hub is enabled on the system; if not, it is disabled.

5.4.3.4 Hub Details > Communications Tab

The following table describes the data that appears on the **Hub Details > Communications** tab.

Field Name	Description
IP address	An eLock hub can be assigned a static IP address or can obtain an IP address via DHCP.
	To use a static IP address, enter the IP address here.
	To use DHCP, enter the NetBIOS name from the sticker on the eLock hub.
Port	The listening port of this eLock hub.
MAC address	The wired MAC address of this eLock hub. This is read from the firmware when ACT Enterprise connects to the eLock hub.
Web Page	If the eLock hub has an on-board web interface, the URL is shown here.

Click **Test Connection** to check that there is a live connection between the database and the eLock hub.

5.4.3.5 Hub Details > Capabilities Tab

This screen shows the hardware capabilities of the eLock hub. For example, the number of doors it can control, the number of users it can support, and the number of I/O modules.

5.4.3.6 Hub Details > Firmware Tab

The **Hub Details > Firmware** tab displays the firmware version on the eLock hub.

5.4.4 Doors

Doors are physical gateways linked to controllers, such as doors, gates, or turnstiles.

ACT Install allows you to add doors to the system and to configure basic properties for their operation.

This section describe the screens and tabs accessed through this menu.

5.4.4.1 Doors Screen

The **Doors** screen shows a list of all doors configured on the system.

The following table describes the search fields and results columns on the **Doors** screen.

Field Name	Description
No	The unique number that identifies this door on the system. (Sortable.)
Door Name	The door's name. Click to view full details for this door on the **Door Details** screen (see *Door Details Screen* on the facing page). (Sortable.)

Field Name	Description
Controller Name	The name of the controller the door is connected to. Click to view full details for this controller on the **Controller Details** screen (see *Controller Details* on page 56). (Sortable.)
Controller	The controller number. (Sortable.)
Local Addr.	The local address for the door at the controller. (Sortable.)
Status	The door's current status. (Sortable.)
Elevator	An elevator icon is shown if the door is connected to an elevator.
Enabled	A green check-mark is displayed for doors that are enabled.

5.4.4.2 Door Details Screen

The **Door Details** screen has a number of tabs showing different settings for the selected door. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Door Details > General Tab* below.
- **OSDP Readers** tab. For more information, see *Door Details > OSDP Readers Tab* below.
- **Timers** tab. For more information, see *Door Details > Timers Tab* on the next page.
- **Operations** tab. For more information, see *Door Details > Operations Tab* on page 67.
- **AUX Relay** tab. For more information, see *Door Details > AUX Relay Tab* on page 68.
- **Reporting** tab. For more information, see *Door Details > Reporting Tab* on page 106.

5.4.4.3 Door Details > General Tab

The following table describes the data that appears on the **Door Details > General** tab.

Field Name	Description
Global Door Number	The door number assigned to the door in the database. This is different to the local door number.
Door Name	The door name.
Controller	The controller the door is connected to.
Local Door Number	The local door number.
Enabled	Whether the door is currently enabled.

Note: Supply voltage to the door can also be reported here. Older controllers do not support reporting of supply voltage.

5.4.4.4 Door Details > OSDP Readers Tab

This tab enables you to configure OSDP readers attached to the current door.

OSDP readers are only supported on door 1 of an ACT1500-family controller.

OSDP readers do not work on controllers without the OSDP jumper.

Click **Add** to add a sub-tab for a new OSDP reader. A sub-tab displays for each OSDP reader.

The following table describes the data that appears on each sub-tab on the **Door Details > OSDP Readers** tab.

Field Name	Description
Address	The address of the reader on the door.
Name	The reader name.
Serial Number	The reader serial number. The serial number is found on the product label, as shown below. **VR10 & VR40** **VR20 & VR50** **Note:** Select the reader type from the drop-down to the right of this area to display an illustration showing the location of the label with the serial number, and the correct jumper position for OSDP.
Direction	Whether the reader controls **Entry** or **Exit**.
Description	A description of the reader.

5.4.4.5 Door Details > Timers Tab

The following table describes the data that appears on the **Door Details > Timers** tab. All times are in seconds.

Field Name	Description
Relay Timer	How long the door relay is activated in response to a valid card or to operation of the request-to-exit (egress) switch.
AUX Output	How long the AUX (buzzer) output is activated when it is fired.
OP2 Timer	How long the OP2 output is activated when it is fired.
OP3 Timer	How long the OP3 output is activated when it is fired.
Door Ajar Timer	How long the door may remain open before a door ajar condition occurs
Extended Relay Timer	How long the door relay is activated in response to a valid card for a user with the **Extended Relay** option. In this case, the door relay is activated for an extended period of time for users who require longer to access the door, for example, wheelchair users. For more information, see *User Details > Options Tab* on page 91.
Tracking Delay Timer	How long the controller waits before updating the count of the number of users in the tracking area.

5.4.4.6 Door Details > Operations Tab

The following table describes the data that appears on the **Door Details > Operations** tab.

Field Name	Description
Door Exit	
Release button	If selected, the push-to-exit (egress switch) is enabled. When this switch is momentarily closed, the relay timer is activated for its programmed period of time, and a user is allowed to exit. An exit event may also be recorded in the system log.
Free exit	Normally, the controller applies the same group access rules to users exiting the area as it applies to users being granted access. If this option is selected, normal access rights are ignored and any enabled card can exit irrespective of time etc.
Exit PINs	Normally in PIN only or PIN & swipe operation, codes are used only to gain entry through the door. If this option is selected, the controller requires a PIN code when exiting also.
Exit PIR	If selected, a Passive Infra-Red (PIR) device can be used in place of a traditional push button exit switch. This ensures that the door remains unlocked while the PIR is active.
Door Security	
Interlock	If selected, only one door of a connected pair may be open at any one time. The interlock output (usually OP3) of each door should be connected to the interlock input (Usually AUX) of the other door. Because this is an electrical interlock, doors on different controllers may be interlocked with each other, or with other devices such as an ACT10 keypad. In this case the 0V lines of all the devices should be connected together.
Toggle Operation	If selected, the door can be toggled open or closed by users with the Toggle Relay option enabled. For more information, see *User Details > Options Tab* on page 91 or *User Group Details > Options Tab* on page 99.
Fail-Safe Relay	When using normally energized locking devices, there may be problems with the door remaining locked during a power outage when a stand-by battery is discharging. If the battery is partially depleted, the voltage may not be high enough to power the controller but may still be producing enough current to keep the solenoid energized. If this option is selected, the action of the relay is reversed so that the door fails open in a power outage.
Intruder Panel	The AUX input on the door may be connected to an Intruder Panel. When this signal is low, the controller knows the panel is armed and denies access to users. This is a secure way of ensuring that the panel is actually armed. The panel may be armed by users with the Arm/Disarm option.
Anti-tailgate	Normally when a card is swiped, the relay is activated for a pre-determined period of time. During this period, the door may be physically opened and closed any number of times as the locking mechanism is disengaged. If this option is selected, the relay time is truncated to one second when the door is opened. This means that the locking mechanism re-engages so the door cannot be reopened without swiping another card.
Break Glass	If selected, the output relay is activated when the glass is broken on a Break Glass Monitor.
Access only	If selected, the main relay output at the access point is activated if a valid card is presented at an access reader. For an exit reader at the access point, ensure that **Exit Granted** is selected under **Door Details > AUX Relay** (see *Door Details > AUX Relay Tab* on the next page) to activate the AUX relay on an exit event.

Field Name	Description
Airlock	If selected, the main relay output is normally activated, and when the door contact closes, the AUX relay is automatically fired. **Note:** This functionality is only supported on an ACT4000 controller with local doors.
Lockdown Reader	If selected, the readers attached to this door function as lockdown readers. For more information on configuring and using lockdown functionality, see *Configure and implement system lockdowns* on page 33. **Note:** Lockdown readers should be used exclusively for lockdown purposes, and never as regular readers, to avoid accidental initiation or clearing of a lockdown.
Bollard	If selected, the AUX relay fires if the door contact is closed. **Note:** This functionality is only supported on an ACT4000 controller with local doors.
Door Buzzer	
Silent operation	Normally the door controller gives an audible success or fail indication when a card is swiped, in addition to activating the red or green indicator on the reader. If this option is selected, this audible indication is suppressed.
Chime	If this option is selected, the door controller's buzzer sounds momentarily when the door is opened. The buzzer (AUX) output is also activated for a short period of time.
Guest button	When an external keypad is being used to gain entry, this option allows the "Bell" button on the keypad to be used to momentarily fire a guest buzzer connected to the buzzer (AUX) output of the controller.

5.4.4.7 Door Details > AUX Relay Tab

The AUX relay is a programmable output on all door controllers. The various settings below may be enabled to determine the conditions for activating this output. It is an open collector output on the ACT1000 (sometimes called the buzzer output) and is a changeover relay on all other controllers.

The following table describes the data that appears on the **Door Details > Relay** tab.

Field Name	Description
Alarms	
The conditions under which an alarm is triggered.	
Door forced	If selected, the output is activated if the door is opened without being explicitly commanded to open by the controller. This would typically occur if the locking mechanism is bypassed or if the door is physically forced open. It is reset when a valid card is swiped.
Door ajar	If selected, the output is activated if the door has been open for longer than a predetermined period of time. It is reset once the door is closed or when a valid card is swiped.
Access denied	If selected, the output is activated for 2 seconds if an invalid card is swiped.
Exit denied	If selected, the output is activated for 2 seconds if an invalid card is swiped at an exit reader.
Duress code used	If selected, the output is activated if a duress PIN code is entered. This is when a number 1 greater than the valid PIN is entered in PIN Only or PIN & Swipe operation.
Break Glass	If selected, the output relay is activated when the glass is broken on a Break Glass Monitor.

Field Name	Description
Normal Access	
The conditions under which normal access is permitted.	
Access granted	If selected, the output is activated if a valid card is swiped. It remains active while the door relay is active.
Exit granted	If selected, the AUX relay output is activated if a valid card is presented at an exit reader. For an access reader ensure that **Access only** is selected from the **Door Details > Operations** tab (see *Door Details > Operations Tab* on page 67) to activate the main relay on an access event.
Door opened	If selected, the output is activated while the door is open.
Follow main relay	If selected, while the main relay is active, the Aux relay is also active.
Arm Intruder panel	If selected, the AUX relay pulses for the AUX Time when a user with the arm/disarm option presents a valid card or PIN. This output must be wired into an input on the alarm panel which signals arming or disarming (usually called keyswitch). If required, the Arm Intruder Panel output may be toggled instead of pulsed. Turn this option on by setting the AUX output time to zero. For more information, see *Door Details > Timers Tab* on page 66.

5.4.4.8 Door Details > Reporting Tab

Selections on this tab determine which additional events are logged to the door controller's system event log.

The following table describes the data that appears on the **Door Details > Reporting** tab.

Field Name	Description
Alarms	
Door Ajar	A door ajar event is logged if the door has been open for longer than a predetermined period of time.
Door Forced	A door forced event is logged if the door is opened without being explicitly commanded to open by the controller. This would typically occur if the locking mechanism is bypassed or if the door is physically forced open.
Door Tamper	A door tamper event is logged if the door is tampered with, that is, if the door station or controller is opened.
Mains Fault	A mains fault event is logged if the mains supply fails. This should be ticked for any doors with a monitored power supply.
Read Error	A read error event is logged when an incorrect read occurs on an entry or exit reader. An additional error number may be displayed giving further details on the error.
Door Status	
Exit Button Used	An exit granted (push button) event is logged when a user presses the request-to-exit (egress) switch.
Door Opened	A door opened event is logged when the door is physically opened.
Door Closed	A door closed event is logged when the door is physically closed.
Door Contact	A door opened/closed event is logged when the door contact changes.

5.4.5 I/O Modules

The I/O (Input/Output) Module (IOM) is an 8 Input/8 Output device that allows ACT controllers to receive/send signals from/to other electronic equipment. For example, an IOM could be connected to elevator controls, alarm systems or CCTV switching.

A maximum of 4 IOMs can be connected to any single controller, giving control of up to 32 inputs and 32 outputs (relays) per controller (4 times 8).

ACT Install allows you to specify the IOMs that are connected to each controller on the physical network, to enable/disable them and to specify whether or not they should log mains faults.

This section describe the screens and tabs accessed through this menu.

5.4.5.1 I/O Modules Screen

The **I/O Modules** screen shows a list of I/O modules configured on the system.

The following table describes the search fields and results columns on the **I/O Modules** screen.

Field Name	Description
No	The unique number that identifies this module on the system. (Sortable.)
I/O Module Name	The I/O module's name. Click to view full details for this module on the **I/O Module Details** screen (see *I/O Module Details Screen* on the facing page). (Sortable.)
Local Addr.	The local address of the module at the controller it is connected to. (Sortable.)
Controller	The number of the controller the module is connected to. (Sortable.)
Controller Name	The name of the controller the module is connected to. Click to view full details for this controller on the **Controller Details** screen (see *Controller Details* on page 56). (Sortable.)
Status	The module's current status, for example online or offline. (Sortable.)
Enabled	A green check-mark is displayed for modules that are enabled. (Sortable.)
Inputs	Click to view a list of inputs on this I/O module. For more information, see *Inputs Screen* on the facing page.
Outputs	Click to view a list of output on this I/O module. For more information, see *Outputs Screen* on page 72.

Click **Add I/O Module** at the top of this page to open a blank **I/O Module Details** screen from which you can add a new I/O module (see *I/O Module Details Screen* on the facing page).

Select the check box for one or more I/O modules in the list area and click **Delete I/O Module** at the bottom of the screen to delete the selected module(s).

Select the check box for one or more disabled I/O modules in the list area and click **Enable** at the bottom of the screen to enable them.

Select the check box for one or more enabled I/O modules in the list area and click **Disable** at the bottom of the screen to disable them.

Click **Floors** at the bottom of the screen to open the **Elevator Floors** screen, where you can specify which I/O module outputs are connected to elevator floors.

Click **Inputs** at the bottom of the screen to open the **Inputs** screen, where you can view a list of all the inputs on the system (see *Inputs Screen* on the facing page).

Click **Outputs** at the bottom of the screen to open the **Outputs** screen, where you can view a list of all the outputs on the system (see *Outputs Screen* on page 72).

5.4.5.2 I/O Module Details Screen

The following table describes the search fields and results columns on the **I/O Module Details** screen.

Field Name	Description
I/O Module Name	The I/O module's name.
Controller	The controller the module is connected to.
Local Address	The local address of the module at the controller.
Enabled	If selected, the module is enabled.
Mains Fault Report	If selected, the module logs mains faults.

5.4.5.3 Inputs Screen

The **Inputs** screen shows a list of inputs connected to a selected I/O module.

The following table describes each of the columns on the **Inputs** screen.

Column Name	Description
Input Name	The input's name. Click to view full details for this input on the **Input Details** screen (see *Input Details Screen* below). (Sortable.)
I/O No.	The unique number that identifies the I/O module for this input on the system. (Sortable.)
No	The number that identifies this input at the I/O module. (Sortable.)
I/O Module Name	The name of the input's I/O module. Click to view full details for this module on the **I/O Module Details** screen (see *I/O Module Details Screen* above). (Sortable.)
Activates Door	If this input activates a door, the door's name is shown here. (Sortable.)
Activates Output	If this input activates an output, the output's name is shown here. (Sortable.)
Status	The input's status. (Sortable.)

5.4.5.4 Input Details Screen

The **Input Details** screen has a number of tabs showing different settings for the selected I/O module. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Input Details > General Tab* below.
- **Options** tab. For more information, see *Input Details > Options Tab* on the next page.
- **Actions** tab. For more information, see *Input Details > Actions Tab* on the next page.

5.4.5.5 Input Details > General Tab

The following table describes the data that appears on the **Input Details > General** tab.

Field Name	Description
Input Name	The input's name. This name appears in the log when the input changes state.
Timer	The amount of time in seconds that the input must remain in a certain state before the change is reported. This prevents a momentary change in the input from causing a false alarm.

Field Name	Description
Timezone	The time zone during which the input is operational. For more information, see *Time zones* on page 110.

5.4.5.6 Input Details > Options Tab

The following table describes the data that appears on the **Input Details > Options** tab.

Field Name	Description
Normally Open	If selected, the input is in the normal state when the contact is open and active when the contact is closed.
Supervised	If selected, the IOM checks for tampers and shorts across the input contacts.
Logging	If selected, the input is logged while enabled.
Alarm	If selected, an alarm is triggered when this input becomes active.

5.4.5.7 Input Details > Actions Tab

The following table describes the data that appears on the **Input Details > Actions** tab.

Field Name	Description
Activate Output	The selected output is activated when the input activates. When the input deactivates, the output de-activates.
Enable Output	The selected output is enabled when the input activates. When the input deactivates, the output is disabled.
Activate Door	The selected door is activated when the input activates. When the input deactivates, the door de-activates.

5.4.5.8 Outputs Screen

The **Outputs** screen shows a list of outputs connected to a selected I/O module.

The following table describes each of the columns on the **Outputs** screen.

Column Name	Description
Output Name	The output's name. Click to view full details for this output on the **Output Details** screen (see *Output Details Screen* on the facing page). (Sortable.)
No	The number that identifies this output at the I/O module. (Sortable.)
I/O No.	The unique number that identifies the I/O module for this output on the system. (Sortable.)
I/O Module Name	The name of the output's I/O module. Click to view full details for this module on the **I/O Module Details** screen (see *I/O Module Details Screen* on the previous page). (Sortable.)
Follow Door	If this output follows the state of a door, the door's name is shown here. (Sortable.)
Status	The output's status.
Floor	If this output may be used for elevator control, an elevator icon appears here.

5.4.5.9 Output Details Screen

The **Input Details** screen has a number of tabs showing different settings for the selected I/O module. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Output Details > General Tab* below.
- **Options** tab. For more information, see *Output Details > Options Tab* below.
- **Actions** tab. For more information, see *Output Details > Actions Tab* below.

5.4.5.10 Output Details > General Tab

The following table describes the data that appears on the **Output Details > General** tab.

Field Name	Description
Output Name	The output's name. This name appears in the log when the output changes state.
Timer	The amount of time in seconds that the output must remain in a certain state before the change is reported. This prevents a momentary change in the output from causing a false alarm.
Timezone	The time zone during which the output is operational. For more information, see *Time zones* on page 110.

5.4.5.11 Output Details > Options Tab

The following table describes the data that appears on the **Output Details > Options** tab.

Field Name	Description
Logging	If selected, the output is logged while enabled.
Normally On	If selected, the output is in the normal state when the contact is open and active when the contact is closed.
Elevator Floor	If selected, the output may be used for elevator control.

See also:

- *Elevator Groups* on page 114

5.4.5.12 Output Details > Actions Tab

An output may be programmed to follow the state of an input or a door.

If a door is selected on this tab, then as that door opens, the output activates. When the door closes, the output de-activates.

5.4.6 Card Configuration

Card configuration allows you to set parameters for the card codes and formats that are used on your system.

This section describe the screens and tabs accessed through this menu.

5.4.6.1 Card Configuration > Site Code Tab

i	Site code support is a legacy feature in ACT Enterprise and cannot be enabled or configured in new installations.

The following table describes the data that appears on the **Card Configuration > Site Code** tab.

Field Name	Description
Site Code 1	The main site code for the system. The default value is 10-2770-09, which allows use of the standard test card supplied with the controllers. Only cards bearing the site code are recognized by the system without needing to be learned individually. Entering 00-0000-00 disables the primary site code.
Site Code 2	A secondary site code that allows cards from a different installation to be used on this system. Entering 00-0000-00 disables the secondary site code.
Issue	The system issue level for cards on this system. If issue numbered cards are used, then only cards with an issue number equal to or greater than the system issue level are accepted. If issue numbering is not used, this field should be zero.
Offset	If a secondary site code is being used, conflict may arise between identically numbered cards on the two systems. To resolve the conflict, an offset may be specified. This is a number that is added to the card number of any card bearing the second site code. For example, an offset of 1000 would mean that card number 1 on the other system is treated as card 1001 on this system. Using a negative value may be used to lower the card number. The offset may be any number from -32768 to 32767.

Click **Write Card** to write the information to a MIFARE card in an External USB reader.

5.4.6.2 Card Configuration > Format Tab

The following table describes the data that appears on the **Card Configuration > Format** tab.

Field Name	Description
Built-in Formats	
HID 26-bit Wiegand	If cards on your system use one or more of these built-in Wiegand card formats, select the check box for each applicable format.
HID 34-bit Wiegand	Click a format in the **Built-in Formats** list to view details of that format in the **Wiegand Format** area.
HID 35-bit Wiegand	
HID 37-bit Wiegand	
Available Formats	
HID 64-bit Wiegand	This list shows non-built-in card formats.
Vanderbilt 34-bit	Click **Add** to add and configure a custom card formats for your system to this list.
	Click a format in the **Available Formats** list to view details of that format in the **Wiegand Format** area.
Wiegand Format	
Select a format in the **Built-in Formats** list or the **Available Formats** list to view details of that format in the **Wiegand Format** area.	
Name	The name for this card format. Editable for user-defined card formats.
Overall	The overall number of digits on the card. This allows the controller to tell the difference between a custom format card and a standard format card.

Field Name	Description
Site Code	The starting digit and length in digits of the site code. **Note:** Site code support is a legacy feature in ACT Enterprise and cannot be enabled or configured in new installations.
Card Number	The starting digit and length in digits of the card number.
Issue Number	The starting digit and length in digits of the issue number. If issue numbering is not used, this is zero.
Use this format	If selected, the custom card format specified here is used instead of the standard format.
Check built-in formats	If selected, controllers process the standard card formats selected under **Built-in Format** as well as the custom format.

5.4.6.3 Card Configuration > Mifare Format Tab

This tab allows you to configure **Card Type**, **Reader Operation Bits**, **Data Specification**, **Data Sector Configuration** and **MAD Configuration** for MIFARE cards. For more information on these options, please contact your MIFARE card supplier.

5.4.6.4 Card Configuration > AUX Card Memory Tab

The following table describes the data that appears on the **Card Configuration > AUX Card Memory** tab.

Note: This only applies to older ACT controllers.

Field Name	Description
Controller AUX Memory	Older controllers have limited memory and cannot support some feature combinations. The preferred option should be selected from the displayed list.
Allow Multiple Cards per User	If selected, users may have more than one token assigned on the system. Otherwise, users can have only one valid card at a time.

5.4.7 DVRs

DVRs (Digital Video Recorders) allow video data to be recorded and played back. In ACT Enterprise, DVRs may be used to record data from cameras associated with doors.

This section describe the screens and tabs accessed through this menu.

5.4.7.1 DVRs Screen

The following table describes the columns on the **DVRs** screen.

Field Name	Description
ID	The DVR's unique ID in ACT Enterprise.
DVR Name	The DVR's name. Click to view details of the DVR on the **DVR Details** screen (see *DVR Details Screen* on the next page).
DVR Type	The DVR type.
Connection	The IP address and port number for the DVR.

5.4.7.2 DVR Details Screen

The following table describes the data that appears on the **DVR Details** screen.

Field Name	Description
ID	The unique ID of the DVR in ACT Enterprise.
DVR Name	The DVR name.
DVR Type	The DVR type.
IP Address	The IP address of the DVR.
IP Port	The listening port of the DVR.
Authentication	The type of authentication used to communicate with the DVR. Options are: **Basic**, **Windows Default** or **Windows**. This field only appears for Milestone DVRs.
Username Password	The username and password used to authenticate when connecting to the DVR. These fields do not appear if **Windows Default** is selected at **Authentication**. In this case, the credentials of the currently logged in Windows user are used to access the DVR.
Domain	The domain associated with the supplied username and password. This field only appears if **Windows** is selected at **Authentication**.
Test Connection	Click to test the connection to the DVR.

5.4.8 Cameras

Cameras may be associated with doors in ACT Enterprise, allowing monitoring of activity at those doors. They may also be connect to DVRs (Digital Video Recorders), to allow video data from the cameras to be recorded and played back.

This section describe the screens and tabs accessed through this menu.

5.4.8.1 Cameras Screen

The following table describes the columns on the **Cameras** screen.

Field Name	Description
No	The camera's unique number in ACT Enterprise.
Camera Name	The camera name. Click to view details of the camera on the **Camera Details** screen (see *Camera Details Screen* on the facing page).
Camera Address/ID	The IP address for the camera.
DVR Name	The name of the DVR the camera is connected to. Click to view details of the DVR on the **DVR Details** screen (see *DVR Details Screen* above).
Doors	The doors covered by this camera.
Enabled	A green check-mark is displayed for cameras that are enabled.

5.4.8.2 Camera Details Screen

The following table describes the data that appears on the **Camera Details** screen.

Field Name	Description
ID	The camera's unique ID in ACT Enterprise.
Camera Name	The camera's name.
DVR	The DVR the camera is connected to.
Connection Address	The globally unique identifier (GUID) for the camera. This connection address is relevant for Milestone servers only.
Enabled	If selected, the camera is enabled.
Doors	The **Assigned Doors** list shows a list of doors covered by this camera. To assign a door to the camera, select the door's name in the **Unassigned Doors** list and click the right-arrow (**>**). To un-assign a door, select the door's name in the **Assigned Doors** list and click the left-arrow (**<**).

5.4.9 SPC Panels

Vanderbilt SPC is an intrusion detection platform that delivers a modern, powerful security system. SPC offers versatility with its wired and wireless intrusion components, integrated access solutions, and comprehensive alarm management functionality. Through the use of secure cloud services, a dedicated software suite, and end-user apps, SPC is at the forefront of modern intrusion technology. You can add SPC panels to ACT Enterprise through ACT Install, and monitor and command the panels through the ACT SiteMaps tools.

See also:

- *SPC Panels Screen* below
- *SPC Panel Details Screen* on the next page
- *Add an SPC Panel* on page 17

5.4.9.1 SPC Panels Screen

This screen lists summary details for each SPC panel registered in ACT Enterprise.

The following table describes the columns displayed for each registered panel on the **SPC Panels** screen.

Field Name	Description
Id	The unique number that identifies this SPC panel in ACT Enterprise. (Sortable.)
Panel Name	The panel name. Click to view full details for this panel on the **SPC Panel Details** screen (see *SPC Panel Details Screen* on the next page). (Sortable.)
Panel Address	The location of the panel, for example, **London Office**. (Sortable.)
Panel Registration Id	The registration ID for the ATS (alarm transmission system) that connects to ACT Enterprise on the panel. (Sortable.)
Auto Grant Engineer Access	Whether the system is configured to automatically grant engineer access on the SPC panel when required using the user credentials supplied. (Sortable.)

Click **Add SPC Panel** to register another panel in ACT Enterprise. See *Add an SPC Panel* on page 17 for more information.

5.4.9.2 SPC Panel Details Screen

This screen shows details of the selected SPC panel.

The following table describes the information that appears on the **SPC Panel Details** screen.

Field Name	Description
Id	The system-generated unique number that identifies this SPC panel on the system.
Panel Name	The panel name.
Panel Address	The location of the panel, for example, **London Office**.
Panel Registration Id	The registration ID for the ATS (alarm transmission system) that connects to ACT Enterprise on the panel.
Username of a User on the SPC Panel	The user account that will be used to access the SPC panel. **Note:** The panel user account must have **Web Access** enabled.
Update PIN / Password of the User	To update the PIN/password that will be used to access the SPC panel, enter the PIN/password and click **Update**. **Note:** This updates the PIN/password stored in ACT Enterprise. It does not change the PIN/password on the panel. For information on how to change a user PIN/password through the panel web interface or a keypad, refer to the SPC 4xxx/5xxx/6xxx Installation & Configuration Manual.
Reset Panel Encryption Key	An encryption key is used to secure communications between an SPC panel and ACT Enterprise. A default encryption key is set on every SPC panel when it is installed or reset. ACT Enterprise knows this default encryption key and uses it to make an initial connection to the panel. The panel and ACT Enterprise then negotiate a new encryption key to secure all further communications. Click **Reset Encryption Key** to tell ACT Enterprise to use the default encryption key to establish a communications channel with this panel. If you reset the encryption key in ACT Enterprise, you should also reset the encryption key on the panel. After resetting the encryption key, you may need to wait up to 60s for the connection to be renegotiated.

To change any of the stored information about an SPC panel, make the required edits on this screen then click **Save SPC Panel** to update details in ACT Enterprise.

To remove a panel from ACT Enterprise, click **Delete SPC Panel**.

5.5 Tools (ACT Install)

The following sections describe the ACT Install tools available in this menu:

5.5.1 System Synchronise

The System Synchronise Wizard allows you to download the entire database to one or more controllers. Synchronising controllers means that all data entered on the controller directly, via its keypad, is lost. Controllers remain offline during downloads, meaning that they cannot be commanded during this time, nor

can they report events. Door stations have limited functionality during the download. You should only do a download if you are certain it is required.

Follow the on-screen instructions, clicking **Next** between steps and **Finish** at the end.

- **Step 1: Controllers.** This screen indicates whether each controller is up to date or not. Select which controllers you want to download to.

- **Step 2: Downloading.** The progress bar shows the overall progress of the system synchronisation. The message area shows information for each controller.

- **Step 3: Results.** The results of the synchronisation operation are shown: the number of controllers updated and their current statuses.

5.5.2 Validation Wizard

The Validation Wizard allows installers to test selected doors, confirming whether they are connected and responding to commands. Only Controllers and Doors that are enabled and online are shown.

Follow the on-screen instructions, clicking **Next** between steps and **Finish** at the end to leave the Wizard.

- **Step 1: Select Objects.** From the tree structure, which shows a list of controllers and the doors connected to each one, select which doors to test.

- **Step 2: Validation Options.** Select which actions to test during validation. Options are: Door Lock, Door Unlock, Door Pass, and Door Normalize.

- **Step 3: Validation.** The Validation screen shows the validation progress: which doors have been validated, and whether they responded to each selected action.

- **Step 4: Finish.** A summary report of the validation tests appears at the end.

5.6 Reports (ACT Install)

ACT Install allows you to generate a number of reports on ACT Enterprise events according to specific criteria.

The following sections describe the reporting functions available in this menu:

5.6.1 System Status

This screen provides an overview of the statuses of controllers, doors and I/O modules on the system.

This report can be printed or exported using the links at the top-right corner of the screen.

Click the arrow (▷) to the left of a status type to see a list of the components with that status.

5.6.2 System Snapshot

This screen provides an overview of the system's operations.

The panel at the top of the screen shows a list of all controllers, doors and I/O devices with summary information about each device and its current status.

The panel at the bottom of the screen shows a list of recent system events, with the time and location of each event, plus summary details.

This report can be printed or exported using the links at the top-right corner of the screen.

5.7 Settings (ACT Install)

The **Settings** screen allows you to configure preferred settings/values for a range of functions in ACT Install, such as default options for controllers and doors, interface language and event filters.

The following sections describe the settings available through this menu:

5.7.1 The Settings screen

The **Settings** screen has a number of tabs showing different settings for ACT Install. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Settings > General Tab* below.
- **Controller Settings** tab. For more information, see *Settings > Controller Settings Tab* on the facing page.
- **Installation** tab. For more information, see *Settings > Installation Tab* on the facing page.
- **Controllers Security** tab. For more information, see *Settings > Controller's Security Tab* on page 82.
- **Default Options > Door** tab. For more information, see *Settings > Default Options – Door Tab* on page 82.
- **Event Filter** tab. For more information, see *Settings > Event Filter Tab* on page 82.
- **Email Notification** tab. For more information, see *Settings > Email Notification Tab* on page 82.
- **Information** tab. For more information, see *Settings > Information Tab* on page 83.

5.7.2 Settings > General Tab

The following table describes the data that appears on the **Settings > General** tab.

Field Name	Description
Language	The language used in the ACT Install interface.
Export CSV Separator	The separator character used when exporting tabular data from ACT Install. For more information, see *Exporting* on page 13.
Auto Logout Time (mins)	The number of minutes after which an idle DB user/operator is logged out.
Expand Live System treeview by default	If selected, the system tree on the left hand side of the **Live System** screen (see *Live System (ACT Install)* on page 53) is fully expanded by default.

Field Name	Description
Confirm deleting Doors in Controller Details	If selected, operators are prompted to confirm door deletion if they de-select the In DB box for a door on the **Controller Details > Doors** tab (see *Controller Details > Doors Tab* on page 57). This is to prevent accidental deletions.

5.7.3 Settings > Controller Settings Tab

The following table describes the data that appears on the **Settings > Controller Settings** tab.

Field Name	Description
General	
Allow International Characters	Select **Allow International Characters** to allow international characters in the names of controllers. This should only be selected if you are connecting to controllers that correctly display European character sets. If connecting to controllers that display only English characters, leaving this box unchecked prevents unsupported characters from being entered into certain database fields.
Controller	
Download names	If selected, User, Door, Group and Time zone names are transmitted to controllers during a download. This allows controllers to locally display and print the correct names for logged events. On larger systems, selecting this option may significantly increase the time taken to download the database to the system (see *System Synchronise* on page 129).
Global PIN Only	If selected, PIN Only operation is required on the entire system.
Global PIN & Swipe	If selected, PIN & Swipe operation is required for all doors in the system at all times. PIN & Swipe settings may also be set up individually for each door on the system.
Duplicate Global PINS Allowed	If selected, the system can be configured with duplicate user PINs. Each user should have a unique token with a common PIN code.
Wiegand	This option is only supported on older ACT controllers.
PIN length	Select the length of PIN required on controllers.

5.7.4 Settings > Installation Tab

The following table describes the data that appears on the **Settings > Installation** tab.

Field Name	Description
Installation Name	The name of the ACT Enterprise installation.
Installation Notes	A description of the installation. This information is visible in a read-only view to operators of other ACT Enterprise clients.

5.7.5 Settings > Controller's Security Tab

The following table describes the data that appears on the **Settings > Controller's Security** tab in ACT Install.

Field Name	Description
Transmit PIN Codes to Controller	If selected, the installer and operator PIN codes are transmitted to all controllers when downloading the database (see *System Synchronise* on page 129). If not selected, controller PINs must be administered on an individual basis.
Installer	The PIN code required to access the **Installer** menu on the individual controllers. This menu is used to configure the card format and interfacing aspects of the controller. This is normally a six-digit code with a default value of 999999.
Operator	This is the PIN code required to access the **Operator** menu on the individual controllers. This menu is used to configure the access rights of users on the controller. This is normally a six digit code with a default value of 123456.

5.7.6 Settings > Default Options – Door Tab

This screen shows default options for new doors. These may be customised on a per-door basis.

See also:

- *Door Details > Operations Tab* on page 67
- *Door Details > AUX Relay Tab* on page 68
- *Door Details > Timers Tab* on page 66
- *Door Details > Reporting Tab* on page 106

5.7.7 Settings > Event Filter Tab

You may optionally specify an event filter to determine which events are recorded in the memory of individual controllers. If the filter is enabled, only selected events are recorded in the controller log.

The following table describes the data that appears on the **Settings > Event Filter** tab.

Field Name	Description
Enable Filter	If this check box is selected, the filter is enabled.
Events	Which events are logged for controllers.
Log Events from Group	Which door group events are logged for.

5.7.8 Settings > Email Notification Tab

The following table describes the data that appears on the **Settings > Email Notification** tab.

Field Name	Description
SMTP Server Settings	Specify details for the SMTP server ACT Enterprise uses to send notification emails. Select the **Enabled Notification** check box to enable email notifications once all SMTP, address, notification and reporting options are configured. **Note:** You can also configure SMTP settings for report emails sent by ACT Manage. For more information, see *Settings > SMTP Tab* on page 142.
Email Addresses	Specify the From and To email addresses to use on notification emails.

Field Name	Description
Notification Options	Specify details of when and how notifications should be sent. • Email Header – Notifications are sent with this subject. • Email Contact – Notifications include the name specified here. This allows you to specify that messages sent to a shared/generic email address are for the attention of a particular individual. • Timezone – Notifications are sent when this timezone is active. • Notification Language – Notifications are sent in the selected language. • Alert Events – Notifications are sent for the event types selected here.
Door Status Reporting	Select the **Enable** check box to enable the generation and emailing of a door status report, then configure the report properties: 1. Select the **Door Group** for which to generate report. 2. Select the check box for each **Day Of Week** on which to generate a report. 3. Select the time of day at which to generate the report. 4. Select the check box for each door status to include in the report.

To test your settings, click **Send Email**. ACT Enterprise sends a test message to the address specified in the **Email To** field on the **Email Addresses** tab.

Click **Default** to return all email notification settings to ACT defaults.

5.7.9 Settings > Information Tab

The following table describes the data that appears on the **Settings > Information** tab.

Field Name	Description
Client logfiles directory	Specifies the full path to the directory in which log files should be saved.
ACT Install logfile	Specify the full path to the ACT Install log file.
ACT Manage logfile	Specify the full path to the ACT Manage log file.
ACT Monitor logfile	Specify the full path to the ACT Monitor log file.

5.8 Clients (ACT Install)

Click any of the client software options in the **Clients** menu to open the corresponding software module for ACT Enterprise. The selected module opens in front of the current module.

You must have logon access to use each client, and which tasks you can perform depends on the access rights you have been granted.

The following options are available (if you have full access rights) on the ACT Install **Clients** menu.

• **ACT Manage**. For more information, see *About ACT Manage* on page 85.

• **ACT Monitor**. For more information, see *About ACT Monitor* on page 150.

• **ACT Server Client**. For more information, see *About ACT ServerClient* on page 48.

- **ACT SiteMaps Editor**. ACT SiteMaps Editor is a visual designer tool that creates a list of maps from pre-designed graphics that represent infrastructure units of an access control site, and places ACT controlling units (doors, inputs/outputs, etc.) on those maps according to their physical location in the building. For more information, please refer to the online help included in ACT SiteMaps Editor.

- **ACT SiteMaps Monitor**. ACT SiteMaps Monitor is an optional add-on to the ACT Enterprise system. It is a real-time access control tool that provides visual navigation through the system of maps created with ACT SiteMaps Editor, allows you to issue basic commands on access control objects on the maps, and allows you to monitor events and status changes from the ACT system via maps in live mode. For more information, please refer to the online help included in ACT SiteMaps Monitor.

6 ACT Manage Reference

This section describes the following:

See also:

- *Navigating ACT Enterprise client interfaces* on page 11
- *About PINs* on page 13

6.1 About ACT Manage

ACT Manage allows you to manage an installed ACT Enterprise system. You can configure and manage card holders, user groups, door groups, timezones, holidays, and access rights across the system. You can run reports on system activity, including event analysis, audit reports, and user validity and activity.

6.2 The ACT Manage Home screen

The **Home** screen provides quick access to the most frequently used ACT Manage features. Click any of these to be brought directly to the relevant screen:

- **List Users**. For more information, see *The Users screen* on page 87.
- **Add User**. For more information, see *The User Details screen* on page 89.
- **Add Cards**. For more information see, *The Extra Cards screen* on page 127.
- **Add User Group**. For more information, see *The Add User Group screen* on page 102.

- **Add Door Group**. For more information, see *The Add Door Group screen* on page 104.
- **Add Timezone**. For more information, see *The Time Zone Details screen* on page 111.

6.3 Live System (ACT Manage)

The **Live System** screen provides a summary view of the ACT Enterprise system.

- **Doors.** This area shows the status of all doors on the system. Hover over the icon for any door to see its status in a popup. You can issue a command on a door by selecting the box for that door, then clicking **Lock**, **Unlock**, **Pass** or **Normalise** at the bottom of the screen.

  You can use the **View Options** to filter the doors you can see in the panel by several criteria. You can view doors that are Online or Offline, Enabled or Disabled. Or you can choose a specific door group to view (this option filters the recent events displayed also).

- **Recent Events.** This area shows the time, location and summary information for events on the system.

  Click **Pause** to temporarily prevent new events from appearing in this area – this may be of use if there are a high volume of events and you want to read the details for one currently on screen. The **Pause** button turns into a **Continue** button when pressed. Click **Continue** to begin adding live events to this area again.

  You can filter the events you can see by selecting a specific **Door Group** in the **View Options** area.

  You can also print and export information displayed in this area. For more information, see *Printing* on page 13 and *Exporting* on page 13.

  For an event involving a user, such as an **Access Granted** or **Access Denied** event, click the user's name in the **Details** column to view the user's profile on the **User Details** screen. Click the **Back** icon ( ) at the top of the **User Details** screen to return to the **Home** screen.

- **Alarms.** This area shows alarms that have been triggered on the system.

  As with the **Recent Events** area, you can pause, print and export the data shown here.

  Click a value in the **Event** column to view that event on the **Event Details** screen (see *The Event Details screen* on page 151).

  You can also mark an alarm as **Acknowledged**, which indicates that you have seen the alarm details and either taken action, or determined that no action is required. Acknowledged alarms are removed from this area. To acknowledge an alarm, select the box for that alarm, enter a password if necessary, and click **Acknowledge**.

If lockdowns have been enabled and configured, you can initiate and clear lockdowns from this screen as follows:

- To initiate a lockdown, click **Lockdown**. All doors in the door group specified under **Lockdown Doors** on the **Settings > Lockdown** tab in ACT Manage are locked down.
- To cancel a lockdown, click **Clear Lockdown**. All doors return to their previous state.

6.4 Users (ACT Manage)

Users are access control card holders. The system allows you to set up new users and provide their details, including their name, user group, validity periods, PIN numbers (if applicable) and card details.

Different data can be recorded for permanent and temporary users of the system.

The following sections describe the functions available in this menu:

See also:

- *User Groups* on page 96

- *Reports (ACT Manage)* on page 130

6.4.1 The Users screen

The **Users** screen is accessed through the **Manage > Users** menu item in ACT Manage.

See also:

- *Search Fields* on the next page

- *Results* on the next page

The following options are also available on this screen:

- To print the user list, click **Print** (**Print**) to open the **Print** dialog for your computer, from which you can select your preferred printer.

- To export the user list, click **Export** (**Export**), and in the dialog that appears specify the required file name and location, then click **Save**. The file may be opened later in a text editor, or a spreadsheet software such as Microsoft Excel.

- To add a user, click **Add User** (**Add User**). See *Add a user* on page 35.

- To add a visitor (a user that is flagged as a visitor and may require fewer or different details), click **Add Visitor** (**Add Visitor**). See *The Visitor Details screen* on page 94.

Note: You can select the box(es) for one or more users in the search results area, then click **Delete User**, **Enable**, **Disable**, **Set Validity** or **Print Cards** at the bottom of the screen to quickly perform any of these operations on the selected user(s). In the case of **Set Validity**, you are prompted to specify the required start/end date/times for the validity period. In the case of **Print Cards**, you are prompted to specify card properties before printing.

6.4.1.1 Search Fields

Field Name	Description
Search	Enter all or part of the registered name for the user whose record you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**ann**e Murphy", and "Joseph H**ann**".
Advanced. Click **Advanced** to see the following additional search fields. You can use one or more fields to specify your search criteria.	
User Number	Enter the user number. The system returns an exact match if found.
First Name	Enter all or part of the user's first name.
Last Name	Enter all or part of the user's last name.
Group	Select the group to which the user is assigned.
Card number	Enter the card number. The system returns an exact match if found.
State	Select the user state: **Enabled**, **Disabled** or **All** (either).
Selectable field	At the final search field, select one additional user field to search on, and enter matching text.

6.4.1.2 Results

The following table describes each of the columns on the **Users** screen search results area.

Column Name	Description
No.	The unique number that identifies this user on the system. (Sortable.)
Name	The user's name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on the facing page). (Sortable.)
Enabled	A green check-mark is displayed for accounts that are enabled. If an account is enabled, the user's card/PIN is operative, though usage may be restricted by a validity period, if set. If an account is disabled, the user's card/PIN does not work. An account must be both enabled **and** valid for the user's card/PIN to work.
Valid	A green check-mark is displayed for accounts that are valid. A user's account is valid if either the current date and time fall within the set validity period, or if no validity period was set for the user. An account must be both enabled and valid for the user's card/PIN to work.
Group	The group this user is a member of. Click to view full details for this group on the **Group Details** screen (see *User Group Details Screen* on page 98). (Sortable.)
Card number	The user's card number (if applicable).
Last column	The default value displayed in the last column is determined by the **Optional Column** setting on the **Settings > General** tab (see *Settings > General Tab* on page 140), but you can change which user field value is shown using the **Advanced** search settings.

6.4.2 The User Details screen

The following table describes the data that appears on the **User Details** screen in ACT Manage.

Field Name	Description
Photo	If a photo of the user has been added to the system, it appears here.
	Click **Upload Photo** to add a photo of the user to the system. See *The Upload Photo screen* on page 96.
User Number	The user number.
User Name	The user name.
	The user name is made up of the specified **First Name** and **Last Name**, and is displayed in logged event lists and queries. Although the combined name may be up to 65 characters in length, only the first 16 characters are visible locally on the door controller LCD. If the combined name exceeds this length, the first name is automatically abbreviated when downloaded.
User Group	The group this user is a member of.
Status	Whether this user is **Enabled** or **Disabled** on the system.
Manual Login	Click to open the **Manual Login** screen where you can manually log the user in to the system (see *The Manual Login screen* on page 154).
Manual Logout	Click to open the **Manual Logout** screen where you can manually log the user out of the system (see *The Manual Logout screen* on page 154).

Configuration Tabs

A set of tabs on the right of the screen allow you to configure different settings for each user. For more information on these tabs, click the links below.

- **General** tab. For more information, see *User Details > General Tab* below.
- **Details** tab. For more information, see *User Details > Details Tab* on page 91.
- **Options** tab. For more information, see *User Details > Options Tab* on page 91.
- **Door Plans** tab. For more information, see *User Details > Door Plans Tab* on page 91.
- **Extra Rights** tab. For more information, see *User Details > Extra Rights Tab* on page 92.
- **Recent Events** tab. For more information, see *User Details > Recent Events Tab* on page 93.
- **View Doors** tab. For more information, see *User Details > View Doors Tab* on page 93.
- **T&A Integration** tab. For more information, see *User Details > T&A Integration Tab* on page 93.
- **Tenants** tab. For more information, see *User Details > Tenants Tab* on page 94.

6.4.3 User Details > General Tab

The following table describes the data that appears on the **User Details > General** tab.

Field Name	Description
User Number	The unique identifying number of the user on the system.
	A default unique value is assigned when a new record is created. If you want to edit this value, it must be changed before the user record is saved for the first time.

Field Name	Description
First Name	The first name of the user. This is a mandatory field.
Last Name	The surname of the user.
Email	The email address of the user.
Mobile	The mobile phone number of the user.
User Group	The group to which the user is assigned. This is a mandatory field. Click the group's name to see more information on the group. The group a user is assigned to determines the access rights for the user. Each group contains a combination of timezone and door group pairs, which determine the doors the user is allowed through and at what times. **Note:** Settings at the user level override settings for the group the user is assigned to if there is a conflict. For more information, see *User Groups* on page 96.
Enabled	If this check box is selected, the user is enabled on the system; if not, they are disabled.
Cards and PIN	
Cards assigned to the user are listed here. Click the card icon to set up a new card for this user. For more information, see *The Card Add screen* on page 96.	
PIN	**Note:** PINs are only applicable for sites where PINs are used. The user's current PIN is not displayed for security reasons. You can reset a user's PIN here. To delete a PIN, click the **X** at the right of the record. In this case, the default PIN for the user group this user is assigned to becomes their new PIN. To reset a PIN, either enter a PIN in this field, or click **Random** to generate a random PIN. Take note of the new PIN to give to the user. The PIN is only displayed until you click **Save**, then it is hidden. For more information on PINs, see *About PINs* on page 13.
Validity Period	
From	The date from which the user is allowed access. Access is denied to the user before this date. Access is granted to the user after midnight on the **Valid From** date. If the box is unchecked then access is allowed up to the **Valid To** date. Some controllers also support a validity time, as well as date. If you do not specify a validity period, the user is always valid.
To	The last day that access is allowed to the user. After this date, access is denied. If the box is unchecked, then access is allowed indefinitely from the **Valid From** date. Some controllers also support a validity time, as well as date. If you do not specify a validity period, the user is always valid.

Field Name	Description
User Notes	
Enter any additional notes on the user.	

6.4.4 User Details > Details Tab

Ten fields appear on this screen – their names are configurable on a per-system level on the **Settings > User Fields** tab in ACT Manage (see *Settings > User Fields Tab* on page 145). Enter information appropriate for the configured field names. For example, on some systems, you might record a user's car registration, or their mobile phone number.

Click the down arrow to the right of a field to see existing field values for all other users. You can select an existing value from this drop-down list, or enter a new one.

6.4.5 User Details > Options Tab

The following table describes the data that appears on the **User Details > Options** tab.

To enable any of these options for the current user, select the check box for that option. To disable an option, de-select the check box. Settings made here override settings inherited from the user's assigned User Group.

Field Name	Description
Toggle Relay	This option causes the relay to toggle whenever the user is granted access. If the door is in its normal state, it is unlocked, and the green reader LED flashes. The door relay is held open so users have free access. If the door is already unlocked, then it is returned to normal operation. This option may be assigned to individual users or to groups.
Extended Relay	This option causes the door relay to remain active for an extended period of time when access is granted. For more information, see *Door Details > Timers Tab* on page 66.
Activate OP2	This option causes the local OP2 output to be fired for a predetermined period of time whenever the user is granted access. This option may be assigned to individual users or to groups.
Activate OP3	This option causes the local OP3 output to be fired for a predetermined period of time whenever the user is granted access. This option may be assigned to individual users or to groups.
Arm/Disarm	ACT controllers may be integrated with intruder panels. Users with the Arm/Disarm option can toggle the AUX relay output on the controller, which tells the alarm panel to arm or disarm. While the door is armed, no access is permitted until a user with the Arm function disarms the door. Disarming the door toggles the output and disarms the panel. The door returns to normal mode. The AUX output must be programmed as an Arm Intruder Panel output.
Monitor User	Users with this option may be located quickly in the **User Tracking** report (see *User Tracking report* on page 134).
Verify Visually	A user with this option has their photograph pop-up on the screen when they access one of the challenge doors.
Visitor Card	Users with this option are considered as visitors in the system.

6.4.6 User Details > Door Plans Tab

Door plans allow you to assign specific doors with time zones to the user. These are only available for controllers with the right capabilities, including extra memory. Please consult your access control

installer if you want this option made available.

Field Name	Description
Time Zone	Select the time zone for the access you want to assign to the user.
Door Group	Select the door group that contains the door(s) you want to assign to the user.
Available Doors	This list shows all doors available for the selected combination of door group and time zone.
	A green door icon indicates that the user has already been assigned this door, either as part of their user group, or on this page. A red door icon indicates that the user has not been assigned this door.
	To add a door/timezone combination to the **Door Plans** list, select the **Time Zone**, **Door Group** and available door, then click the right-arrow ( ).
	To add access to all doors for the selected time zone/door group combination, click the double-right-arrow ( ).
	Notes:
	• The right-arrow is disabled ( ) until you have selected a time zone, door group and door.
	• Assignments are not updated until you click **Save**.
Door Plans	This list shows the door/time zone combinations assigned to the user.
	To remove access to a time zone/door combination, select it in the **Door Plans** list and click the left-arrow ( ).
	To remove access to all time zone/door combinations, click the double-left-arrow ( ).
Doors assigned already by user group X	This list shows which door/time zone combinations the user already has access rights for, as determined by the first user group they are assigned to.

6.4.7 User Details > Extra Rights Tab

Extra rights allow you to assign up to 16 extra door group and time zone combinations to the user. These are only available for controllers with the right capabilities, including extra memory. Please consult your access control installer if you want this option made available. A user can access an assigned door during the period specified by the corresponding time zone.

Field Name	Description
Time Zone	Select the time zone for extra rights you want to assign to the user.
Validity Period	Optionally specify a period during which these extra rights are valid.

Field Name	Description
Available Door Groups	This list shows all door groups available to the current user. A green door icon indicates that the user has already been assigned this door group, either as part of their user group, or on this page. A red door icon indicates that the user has not been assigned this door group.

To add a door group/time zone combination to the **Extra Rights** list, select the **Time Zone** above and the door group for which the extra right should apply here, then click the right-arrow (▶).

To add access to all door groups for the selected time zone, click the double-right-arrow (▶▶). If there are more than 16 door groups, you see a warning message and only the first 16 are copied across.

Note: The right-arrow is disabled (▷) until you have selected both a time zone and a door group. The double-right arrow is disabled (▷▷) until you have selected a time zone. |
| Extra Rights | This list shows all extra rights assigned to the current user.

To remove access to a time zone/door group combination, select it in the **Extra Rights** list and click the left-arrow (◀).

To remove access to all time zone/door group combinations, click the double-left-arrow (◀◀). |
| Rights already provided by user group | This panel lists the access rights (door groups and time zones) the user has due to their assigned user group. |

6.4.8 User Details > Recent Events Tab

This tab displays a list of recent events for the user.

Field Name	Description
Time	The time of the event.
Event	The event.
Location	The location (door or barrier) of the event.
Details	Details of the event.

6.4.9 User Details > View Doors Tab

This tab shows a list of door/time zone combinations valid for this user.

A user can only access a door during the period specified by the associated time zone.

The **Source** column indicates the primary source of each door/time zone combination. This may be the user's User Group, Extra Rights, or Door Plan.

6.4.10 User Details > T&A Integration Tab

This tab is disabled unless time and attendance (T&A) integration with a third party system is enabled and configured in ACT Manage under **Settings > T&A Integration** (see *Settings > T&A Integration Tab* on page 147).

ACT Enterprise can also generate a basic T&A report, based on events at entry and exit doors in the system. For more information on T&A options in ACT Enterprise, see *Report on time and attendance (T&A)* on page 45.

To configure T&A settings for this user:

1. Select whether the user should **Use user group default settings** for whether or not T&A data is recorded, or whether T&A should be explicitly **Enabled** or **Disabled** for this user. For more information on configuring T&A settings for a user group, see *User Group Details > T&A Integration Tab* on page 101.

2. At **T&A Doors**, select the door group that includes the entry and exit readers used to determine when this user is considered logged in/out for T&A purposes.

   If no user-specific door group is selected, the door group selected at **Settings > T&A Integration > Options > T&A Doors** is used by default.

3. Click **Save**.

6.4.11 User Details > Audit Details Tab

This tab shows the first and last log events for the user, plus the date on which the user was created in ACT Enterprise and the DB user that created the user. The log events displayed on this screen are stored in the user record in the database and are not affected by purges of the system log.

6.4.12 User Details > Tenants Tab

This tab shows a list of the tenancies to which the user is assigned.

See also:

- *Tenancy* on page 121

6.4.13 The Visitor Details screen

This screen displays when you are adding a visitor user to the system.

Field Name	Description
Photo	Click **Upload Photo** to add a photo of the user to the system. See *The Upload Photo screen* on page 96.
User Name	Displays the user's full name once **First Name** and **Last Name** have been saved.
	The user's name is made up of the specified **First Name** and **Last Name**, and is displayed in logged event lists and queries. Although the combined name may be up to 65 characters in length, only the first 16 characters are visible locally on the door controller LCD. If the combined name exceeds this length, the first name is automatically abbreviated when downloaded.
User Group	Displays the group this user is a member of once **User Group** has been saved.
Status	Whether this user is **Enabled** or **Disabled** on the system.
General	
First Name	Enter the user's first name.
Last Name	Enter the user's surname.
User Group	Select the group to which the user should be assigned. Click **View** to see more information on the selected group.
	The group a user is assigned to determines the access rights for the user. Each group contains a combination of timezone and doorgroup pairs, which determine the doors the user is allowed through and at what times.
	For more information, see *User Groups* on page 96.

Field Name	Description
Enabled	Select this check box if the user's card has been issued and they can be enabled on the system. Otherwise, de-select this check box.
Cards and PIN	
One-To-One Card	Click the card icon to set up a new card for this user. For more information, see *The Card Add screen* on the next page.
PIN	To set a PIN for the user, either enter a PIN in this field, or click **Random** to generate a random PIN. Take note of the new PIN to give to the user. The PIN is only displayed until you click **Save**, then it is hidden.
Validity Period	
From	Specify the date from which the user is allowed access. Access is denied to the user before this date. Access is granted to the user after midnight on the **Validity Period From** date. If the box is unchecked then access is allowed up to the **Validity Period To** date. Some controllers also support a validity time, as well as date.
To	Specify the last day that access is allowed to the user. After this date, access is denied. If the box is unchecked, then access is allowed indefinitely from the **Validity Period From** date. Some controllers also support a validity time, as well as date.

6.4.14 The Print Cards screen

The following table describes the data that appears on the **Print Cards** screen in ACT Manage.

Field Name	Description
Users to print cards for	Select the check box for each user you want to print a card for.
Card	Select the type of card you want to print. A preview of the card type is shown.
Flip Card Side	Click to view the alternate card side in the preview.
Print both sides Print active side only	Select whether to **Print active side only** (the side you are currently previewing) or **Print both sides**.
Encoding Profile	Select which encoding profile to use when printing the card(s).
Barcode Profile	Select which barcode profile to use when printing the card(s).

6.4.15 The Upload Photo screen

The following table describes the data that appears on the **Upload Photo** screen in ACT Manage.

Field Name	Description
Source Type	Select the photo source: - **File** – Click **Open** to open a dialog where you can browse for and select the image file to use. Photos must be in JPG, GIF, BMP, PNG or TIFF format. ACT Enterprise resizes images and converts files to JPG format during import. - **Video** – Select the **Video Source** from the drop-down provided, then click **Capture** to take a picture. - **Twain** – Click **Acquire** to scan the image.
Source	Shows the full original image opened/captured/acquired. You can click and drag to select a cropped area of the image to use as the final user photo.
Preview	Shows the final user photo. This is either the full or cropped image from the **Source** area. Click **Apply** to save.

6.4.16 The Card Add screen

When adding a card for a user (see *User Details > General Tab* on page 89), this screen allows you to specify a source from which to read the number of a presented card. Select the source type, then the specific source and click **Capture** to read the card number. Click **Save** to return to the **User Details > General** tab with the card number now populated.

6.4.17 The Copy User screen

The following table describes the data that appears on the **Copy User** screen.

Field Name	Description
Copy To	Specify the start and end range of users you want to copy selected details to. If the users already exist, their current details are overwritten. If they do not already exist, users with the copied details are created. You should verify whether or not user IDs in the specified range are already in use before you copy user details.
Items to copy	Select the check box for each property from the selected user you wish to copy to the specified existing/new users.
Enable new users	Select this check box to enable any new users created by the operation.
Visitor cards	Select this check box to assign visitor cards for any new users created by the operation.

Click **Apply** to copy details to new/existing users.

6.5 User Groups

User groups are used to define common settings and access rights for a set of users.

When you create a user profile, you select one user group to which the user belongs (see *User Details > General Tab* on page 89), and their access rights are those assigned to that group. If the group's rights change, then so do those of all members of the group.

If required, users can be assigned additional access rights on the **User Details > Extra Rights** tab (see *User Details > Extra Rights Tab* on page 92).

The following sections describe the functions available in this menu:

See also:

- *Users (ACT Manage)* on page 86

- *The Users screen* on page 87

- *The User Details screen* on page 89

6.5.1 The User Groups screen

The following table describes the search field and results columns on the **User Groups** screen.

Note: All user groups are displayed on this screen at the same time, with no pagination.

Field Name	Description
Search	Enter all or part of the name of the group you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Team" might show results for "**Team** A", "Security **Team**", and "S**team** Cleaner Operators".
No	The unique number that identifies this group on the system. (Sortable.)
Name	The group's name. Click to view full details for this user on the **Group Details** screen (see *User Group Details Screen* on the next page). (Sortable.)
Enabled	A green check-mark is displayed for groups that are enabled. (Sortable.)
Number of Users	The number of users in the group. Click to see a list of users in this group on the **Users** screen (see *The Users screen* on page 87). (Sortable.)
Access Rights	The first door group/time zone combination assigned to this group. Up to 8 combinations may be assigned per group. To view all access rights assigned, view the **User Group Details > Access Rights** tab (see *User Group Details > Access Rights Tab* on page 99). (Sortable.)
Elevator Group	The elevator group assigned to this group on the **User Group Details > General** tab (see *User Group Details > General Tab* on the next page). (Sortable.)

Click **Add User Group** at the top of this page to open a blank **Group Details** screen (see *User Group Details Screen* on the next page) from which you can add a new user group.

Select the check box for one or more user groups in the list area and click **Delete User Group** at the bottom of the screen to delete the selected user group(s).

6.5.2 User Group Details Screen

The **User Group Details** screen has a number of tabs showing different settings for the selected group. For more information on these tabs, click the links below.

- **General** tab. For more information, see *User Group Details > General Tab* below.

- **Access Rights** tab. For more information, see *User Group Details > Access Rights Tab* on the facing page.

- **Options** tab. For more information, see *User Group Details > Options Tab* on the facing page.

- **Default Card** tab. For more information, see *User Group Details > Default Card Tab* on page 100.

- **Anti-passback** tab. For more information, see *User Group Details > Anti-passback Tab* on page 100.

- **Area Limits** tab. For more information, see *User Group Details > Area Limits Tab* on page 101.

- **View Doors** tab. For more information, see *User Group Details > View Doors Tab* on page 101.

- **T&A Report** tab. For more information, see *User Group Details > T&A Report Tab* on page 101.

- **Tenants** tab. For more information, see *User Group Details > Tenants Tab* on page 101.

Click **Add User Group** at the bottom of this page to open a blank **User Group Details** screen from which you can add a new user group.

6.5.3 User Group Details > General Tab

The following table describes the data that appears on the **User Group Details > General** tab.

Field Name	Description
User Group Number	The user group's unique identifying number on the system. This is a unique number between 1 and 1024.
	A default unique value is assigned when a new record is created. If you want to edit this value, it must be changed before the user group record is saved for the first time.
User Group Name	The user group's name.
	This is a mandatory field.
	The name may be up to 32 characters in length, but only the first 16 characters are visible locally on the door controller LCD.
Elevator Group	The elevator group to which this user group is assigned. This determines which floors members of the user group can access, and at what times.
	For more information, see *Elevator Groups* on page 114.
	Click **Elevators** to go to the **Elevator Manager** screen (see *The Elevator Manager screen* on page 115).

Field Name	Description
PIN	The PIN code for users in this group if they have not been assigned an individual user PIN. PINs must be unique for user groups. For more information on PINs, see *About PINs* on page 13. **Note:** PINs only need to be assigned for systems requiring Card & PIN usage. The user group's current PIN is not displayed for security reasons. You can delete or reset a user group's PIN here. To delete a PIN, click the **X** at the right of the record. To reset a PIN, either enter a PIN in this field, or click **Random** to generate a random and unique PIN. Take note of the new PIN. The PIN is only displayed until you click **Save**, then it is hidden.
Enabled	If this check box is selected, the user group is enabled on the system; if not, it is disabled.

6.5.4 User Group Details > Access Rights Tab

This tab shows the access rights for users in this User Group. Up to 8 combinations of Door Group and Time Zone can be assigned for each User Group.

Users can only access each specified door group when the corresponding time zone is active.

See also:

- *Door Groups* on page 102
- *Time zones* on page 110

6.5.5 User Group Details > Options Tab

The following table describes the data that appears on the **User Group Details > Options** tab.

To enable any of these options for the current user group, select the check box for that option. To disable an option, de-select the check box.

Field Name	Description
Toggle Relay	This option causes the relay to toggle whenever a user in this group is granted access. If the door is in its normal state, it is unlocked, and the green reader LED flashes. The door relay is held open so users have free access. If the door is already unlocked, then it is returned to normal operation. **Note:** A different setting on the **User Details > Options** tab overrides the setting at group level (see *User Details > Options Tab* on page 91).
Activate OP2	This option causes the local OP2 output to be fired for a predetermined period of time whenever a user in this group is granted access. **Note:** A different setting on the **User Details > Options** tab overrides the setting at group level (see *User Details > Options Tab* on page 91).
Activate OP3	This option causes the local OP3 output to be fired for a predetermined period of time whenever a user in this group is granted access. **Note:** A different setting on the **User Details > Options** tab overrides the setting at group level (see *User Details > Options Tab* on page 91).

Field Name	Description
Tracking Bypass	This option allows tracking functions to be bypassed for users in this group. This means that anti-passback, user-limiting and random challenge functions do not apply to users in this group.
	This option also allows users in this group to access/exit locked down doors during a lockdown if the **Allow access/exit to User Groups with Bypass** option set is enabled on the **Settings > Lockdown** tab (see *Settings > Lockdown Tab* on page 142).
Lockdown	This option allows users in this group to initiate and clear lockdowns from a card reader.
	To initiate a lockdown, a user should present their card once at a designated lockdown reader.
	To clear a lockdown, a user should present their card twice in rapid succession at a designated lockdown reader.
	A reader is designated a lockdown reader on the **Door Details > Operations** screen in ACT Install. See *Door Details > Operations Tab* on page 67.

See also:

- *User Details > Options Tab* on page 91

6.5.6 User Group Details > Default Card Tab

This tab shows the card designs available, and allows you to choose the default card design for members in this group.

To view any of the card designs in greater detail, click **Full Size** beside the card image. Click **Back** on the **Card** screen to return to the **Group Details > Default Card** tab.

To select a default card design for this User Group, select the radio button beside the design, then click **Save**.

To permanently delete a card design, select the radio button beside the design, then click **Delete**.

6.5.7 User Group Details > Anti-passback Tab

The anti-passback feature is designed to stop users giving their cards to other users seeking to gain access to an area. It does this by requiring users to exit an area before re-entry is granted.

When a user is granted access through a timed anti-passback door, then the user is not granted access again, until either:

- the anti-passback time period expires

  or

- the user exits.

The anti-passback period can be set from 0 days, 0 hours and 0 minutes, up to 7 days, 23 hours and 59 minutes. The anti-passback period has resolution of one minute.

To disable anti-passback, set the time to 0 days, 0 hours 0 minutes.

To enable anti-passback, set the time to any other value in the allowed range.

Timed anti-passback only functions on doors which are configured as timed anti-passback doors. Anti-passback doors can be configured in ACT Manage under **Settings > Doors**. For more information, see *Settings > Doors Tab* on page 141.

> Antipassback data may be automatically cleared down at a specific time daily if **Muster Cutoffs** are configured in ACT Manage under **Settings > Muster Report**. For more information, see *Settings > Muster Report Tab* on page 143.

6.5.8 User Group Details > Area Limits Tab

User Group Area Limits allow you to restrict how many users from a user group can access a defined area at one time. This may be useful, for example, to restrict access to a car park according to the number of available parking spaces.

The User Group limit should be lower than the overall area limit. Once the group limit is reached, no more users from that group can enter the area until a member of the group leaves. Users from other groups may still enter the area until the overall area limit is reached.

Areas are defined by assigning a door group under the **Settings > Area Limits** tab (see *Settings > Area Limits Tab* on page 145). When a valid user enters one of the doors in the door group, the count increments. The count is decremented when a card holder leaves through one of the doors in the door group. When a limit is reached, access is denied to the next user who tries to access the area.

Notes:

- Entry and Exit readers are required on the doors for this feature to work.
- Only users explicitly entering and exiting with their cards can be counted.

See also:

- *Settings > Area Limits Tab* on page 145

6.5.9 User Group Details > View Doors Tab

This tab shows a list of door/time zone combinations valid for users assigned to this user group.

See also:

- *Doors (ACT Manage)* on page 104

6.5.10 User Group Details > T&A Report Tab

This tab shows configuration settings that determine how normal and overtime hours are calculated for users assigned to this user group when reporting on T&A (time and attendance) in ACT Enterprise. For information on T&A reports, see *Time and Attendance report* on page 137.

> It is also possible to integrate ACT Enterprise with a third party T&A system. For more information on T&A options in ACT Enterprise, see *Report on time and attendance (T&A)* on page 45.

To specify the criteria for normal and overtime hours for users in this group, either:

- Select the timezones that cover the **Normal Hours** and **Overtime Hours** for users in this user group. For more information on timezones, see *Time zones* on page 110.

  or

- Specify the maximum number of normal and overtime hours that users in this user group can work each day.

6.5.11 User Group Details > Tenants Tab

This tab shows a list of the tenancies to which the user group is assigned.

See also:

- *Tenancy* on page 121

6.5.12 User Group Details > T&A Integration Tab

This tab is disabled unless time and attendance (T&A) integration with a third party system is enabled and configured in ACT Manage under **Settings > T&A Integration** (see *Settings > T&A Integration Tab* on page 147).

ACT Enterprise can also generate a basic T&A report, based on events at entry and exit doors in the system. For more information on T&A options in ACT Enterprise, see *Report on time and attendance (T&A)* on page 45.

To configure default T&A settings for users assigned to this user group:

1. Select the **Enable T&A Integration** check box if users in this user group should have T&A data tracked by default.

2. Select the **Apply T&A Integration to existing users** check box to create linked accounts in the T&A system for all current users in ACT Enterprise.

   Accounts are created automatically for new users added to ACT Enterprise after T&A integration is enabled.

3. Click **Save**.

6.5.13 The Add User Group screen

This wizard allows you to add a door group to the system by following these steps:

- **Step 1: User Group Details.**
- **Step 2: Access Rights.** Select the doors you want to add to the group from the **Available Doors** list and click the right-arrow ( ) to add them to the **Doors in Group** list. You can use the **Search** field at the top of the list to locate a particular door if you know its name. When you have added all required doors, click **Next**.
- **Step 3: User Group Options.** A summary of the door group you created is shown. Click **Finish**.
- **Step 4: Results.** A summary of the door group you created is shown. Click **Finish**.

6.6 Door Groups

Door groups are a convenient way of grouping a number of doors to simplify granting/denying access to that group of doors.

The following sections describe the functions available in this menu:

6.6.1 The Door Groups screen

The **Door Groups** screen shows a list of all the door groups configured on the system.

Field Name	Description
No	The unique number that identifies this door group on the system. (Sortable.)
Name	The door group's name. Click to view full details for this user on the **Door Group Details** screen (see *The Door Group Details screen* on the facing page). (Sortable.)
Number of Doors	The number of doors in the group. (Sortable.)

Click **Add Door Group** at the top of this page to open a blank **Door Group Details** screen (see *The Door Group Details screen* below) from which you can add a new door group.

Select the check box for one or more door groups in the list area and click **Delete Door Group** at the bottom of the screen to delete the selected door group(s).

6.6.2 The Door Group Details screen

The **Door Group Details** screen has two tabs showing different settings for the selected door group. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Door Group Details > General Tab* below.
- **User Groups** tab. For more information, see *Door Group Details > User Groups Tab* below.
- **Tenants** tab. For more information, see *Door Group Details > Tenants Tab* below.

Click **Add Door Group** at the bottom of this page to open a blank **Door Group Details** screen from which you can add a new user group.

6.6.3 Door Group Details > General Tab

The following table describes the data that appears on the **Door Group Details > General** tab.

Field Name	Description
Door Group Number	The door group's unique identifying number on the system. A default unique value is assigned when a new record is created. If you want to edit this value, it must be changed before the door group record is saved for the first time.
Door Group Name	The door group's name. The name may be up to 32 characters in length, but only the first 16 characters are visible locally on the door controller LCD.
Available Doors	This list shows all doors available to be added to this door group. Click a door name to view details of that door on the **Door Details** screen (see *The Door Details screen* on the next page). To add a door to the **Doors in Group** list, select the door in this list, then click the right-arrow ( ). To add all doors, click the double-right-arrow ( ). **Note:** The right-arrow is disabled ( ) until you have selected a door.
Doors in Group	This list shows the doors in this door group. Click a door name to view details of that door on the **Door Details** screen (see *The Door Details screen* on the next page). To remove a door, select it in the **Doors in Group** list and click the left-arrow ( ). To remove all doors, click the double-left-arrow ( ).

6.6.4 Door Group Details > User Groups Tab

The **Door Group Details > User Groups** tab shows which user groups the current door group is assigned to. Click a user group **Name** to view details of the user group on the **User Group Details** screen. See *User Group Details Screen* on page 98.

6.6.5 Door Group Details > Tenants Tab

This tab shows a list of the tenancies to which the door group is assigned.

See also:

- *Tenancy* on page 121

6.6.6 The Add Door Group screen

This wizard allows you to add a door group to the system by following these steps:

- **Step 1: Door Group Details.** Enter a **Door Group Name** and click **Next**.

- **Step 2: Assign Doors.** Select the doors you want to add to the group from the **Available Doors** list and click the right-arrow (▶) to add them to the **Doors in Group** list. You can use the **Search** field at the top of the list to locate a particular door if you know its name. When you have added all required doors, click **Next**.

- **Step 3: Results.** A summary of the door group you created is shown. Click **Finish**.

6.7 Doors (ACT Manage)

Doors are physical gateways linked to controllers, such as doors, gates, or turnstiles.

ACT Manage allows you to view a list of all doors configured on the ACT Enterprise system and to configure certain, limited properties for those doors. Adding and managing doors is mainly done through ACT Install. For more information, see *About ACT Install* on page 53.

The following sections describe the functions available in this menu:

6.7.1 The Doors screen

The **Doors** screen shows a list of doors configured on the system.

Field Name	Description
No	The unique number that identifies this door on the system. (Sortable.)
Name	The door's name. Click to view full details for this user on the **Door Details** screen (see *The Door Details screen* below). (Sortable.)
Enabled	A green check-mark is displayed for doors that are enabled. (Sortable.)

6.7.2 The Door Details screen

The **Door Details** screen has a number of tabs showing different settings for the selected door. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Door Details > General Tab* on the facing page.

- **Door Groups** tab. For more information, see *Door Details > Door Groups Tab* on the facing page.

- **Actions** tab. For more information, see *Door Details > Actions Tab* on the facing page.

- **Reporting** tab. For more information, see *Door Details > Reporting Tab* on page 106.

- **Floor Group** tab. For more information, see *Door Details > Floor Group Tab* on page 107.

- **Tenants** tab. For more information, see *Door Details > Tenants Tab* on page 107.

6.7.3 Door Details > General Tab

The following table describes the data that appears on the **Door Details > General** tab.

Field Name	Description
Door Number	The door's unique identifying number on the system.
Door Name	The door's name. The name may be up to 32 characters in length, but only the first 16 characters are visible locally on the door controller LCD.
Relay Timer	How long in seconds the door relay is activated in response to a valid card or to operation of the request-to-exit (egress) switch.
Door Ajar Timer	How long in seconds the door may remain open before a door ajar condition occurs.

6.7.4 Door Details > Door Groups Tab

The **Door Details > Door Groups** tab shows which door groups the current door belongs to.

The **Available Door Groups** list shows a list of door groups to which the current door does not belong, and the **Door member of** list shows the door groups to which they do belong. Click a door group name to view details of that door group on the **Door Group Details** screen (see *The Door Group Details screen* on page 103).

To add the door to a door group, select the required group in the **Available Door Groups** list, then click the right-arrow (▶).

To remove the door from a door group, select the required group in the **Door member of** list, then click the left-arrow (◀).

6.7.5 Door Details > Actions Tab

Actions are settings automatically applied by a door controller at specified times without the need for user intervention. They may be used to control external devices via the controller outputs, or to alter the security level of a door at certain times. Each action may be inactive (default) or have any defined time zone assigned.

The following table describes the data that appears on the **Door Details > Actions** tab.

For each available action, select a time zone from the corresponding drop-down list to determine when the action applies for this door.

Field Name	Description
Unlock Door	The time zone assigned to this action determines when the door is automatically unlocked. When a door is unlocked, users have free access without needing to swipe a card. The door relay is held open for this time, and the green reader LED flashes.
Lock Door	The time zone assigned to this action determines when the door is automatically locked. When a door is locked, all users are denied access irrespective of their programmed access rights. The door relay is held closed for this time, and the red reader flashes.
PIN Required	The time zone assigned to this action determines when Card and PIN operation is in force on the door. When a card is presented during this time, a valid user or group PIN must be entered to gain access.

Field Name	Description
Any Card	The time zone assigned to this action determines when **any** proximity/magnetic stripe card are allowed access. The only check performed is that a card is presented: the format is irrelevant. **Example:** This could be used to allow access to a bank ATM lobby to anybody with a magnetic stripe card.
OP2 Active	The time zone assigned to this action determines when the OP2 output is active. This could be used to control an externally connected device.
OP3 Active	The time zone assigned to this action determines when the OP3 output is active. This could be used to control an externally connected device.
AUX Active	The time zone assigned to this action determines when the AUX output is active. This could be used to control an externally connected device.
PIN Only	The time zone assigned to this action determines when PIN Only operation is in force for the door. During this time, all card swipes are ignored, and a valid user PIN must be entered to gain access.
PIN or Card	The time zone assigned to this action determines when either a valid PIN or Card operation is required to gain entry. During this time, any valid card or PIN must be entered to gain access.
Twin Users	The time zone assigned to this action determines when two valid cards must be presented to gain access. This is typically used in high security applications where two people must be in the room at the same time.
Normalise Doors	The time zone assigned to this action determines when the door is normalised. That is, the door returns to its default state.

See also:

- *Time zones* on page 110

6.7.6 Door Details > Reporting Tab

Selections on this tab determine which additional events are logged to the door controller's system event log.

The following table describes the data that appears on the **Door Details > Reporting** tab.

Field Name	Description
Alarms	
Door Ajar	A door ajar event is logged if the door has been open for longer than a predetermined period of time.
Door Forced	A door forced event is logged if the door is opened without being explicitly commanded to open by the controller. This would typically occur if the locking mechanism is bypassed or if the door is physically forced open.
Door Tamper	A door tamper event is logged if the door is tampered with, that is, if the door station or controller is opened.
Mains Fault	A mains fault event is logged if the mains supply fails. This should be ticked for any doors with a monitored power supply.

Field Name	Description
Read Error	A read error event is logged when an incorrect read occurs on an entry or exit reader. An additional error number may be displayed giving further details on the error.
Door Status	
Exit Button Used	An exit granted (push button) event is logged when a user presses the request-to-exit (egress) switch.
Door Opened	A door opened event is logged when the door is physically opened.
Door Closed	A door closed event is logged when the door is physically closed.
Door Contact	A door opened/closed event is logged when the door contact changes.

6.7.7 Door Details > Floor Group Tab

If this door is being used as a reader in an elevator, then this tab shows the floor group that specifies all the floors the elevator cab is allowed access to.

To assign this door to a floor group, select the appropriate floor group from the drop-down list provided and click **Save**.

See also:

- *Elevator Groups* on page 114
- *Elevator Manager > Floor Groups Tab* on page 116

6.7.8 Door Details > Tenants Tab

This tab shows a list of the tenancies to which the door is assigned.

See also:

- *Tenancy* on page 121

6.8 Rules

Rules enable you to automate the ACT Enterprise system to take one or more specific actions in response to log events.

For example, you could configure the system to:

- Send an email when a banned user tries to use their access card to enter the building.
- Activate an I/O unit to activate an alarm or floodlight if a door is forced during the night.
- Lock a specific door and turn off outputs controlling lights when a certain user exits the building.

For rules to be triggered, the server must be running, and controllers must be connected and issuing log events.

The following sections describe the functions available in this menu:

See also:

- *Add a rule* on page 46

6.8.1 The Rules screen

The **Rules** screen is accessed through the **Manage > Rules** menu item in ACT Manage.

The following options are also available on this screen:

- To print the rules list, click **Print** to open the **Print** dialog for your computer, from which you can select your preferred printer.

- To export the rules list, click **Export**, and in the dialog that appears specify the required file name and location, then click **Save**. The file may be opened later in a text editor, or a spreadsheet software such as Microsoft Excel.

- To add a rule, click **Add Rule**. See *Add a rule* on page 46.

Note: You can select the box(es) for one or more rules in the search results area, then click **Delete Rule**, **Enable** or **Disable** at the bottom of the screen to quickly perform any of these operations on the selected rule(s).

The following table describes each of the columns on the **Rules** screen search results area.

Column Name	Description
No.	The unique number that identifies this rule on the system. (Sortable.)
Enabled	A green check-mark is displayed for rules that are enabled.
Name	The rule name. Click to view full details for this rule on the **Rule Details** screen (see *The Rule Details screen* below). (Sortable.)
Total Activations	The total number of times this rule has been triggered on the system. Checking the number of **Total Activations** of a rule may provide an indication that a given rule is triggering at an unexpected rate, whether too high or too low.
Last Date Activated	When the rule was last triggered.
Creation	When the rule was created.

6.8.2 The Rule Details screen

The following table describes the **Rule Details** screen in ACT Manage.

Field Name	Description
Rule Name	The rule name.
Rule configuration area	This area displays the rule as a flow diagram. To add a rule element, right-click and select **New Analyser**, **New Logic**, or **New Action**, then configure the element as required. To connect elements together in the required sequence, drag the black circle from the top-right of an **Analyser** or **Logic** box to a **Logic** or **Action** box. Use analysers to identify rule triggers; optionally, combine analysers using logic operations; then specify the action(s) the system should perform when the rule is triggered. For information on how to configure rules, see *Add a rule* on page 46.

6.8.2.1 Analyser types

Supported analyser types are described below.

Remember that an analyser can be used to trigger a rule when it is evaluated as TRUE, or can be used with NOT logic to trigger a rule when it is evaluated as FALSE. For example, you could configure a rule to

be triggered by an event on a specific door, or to be triggered by an event on *any other door, but not this one*.

Analyser Type	Description
Door	Select a door for which the rule should apply.
Door group	Select the door group for which the rule should apply.
User search	Enter the full/partial **Surname** and/or **Firstname** of the user(s) for which the rule should apply. For example, entering "Ann" in the **Firstname** field will match "**Ann**-Marie Boyle" and "Jo**anne** Murphy". Wildcards are not supported.
User group	Select the user group for which the rule should apply.
Timezone	Select the timezone for which the rule should apply.
Event type	Select the specific event type for which the rule should apply.
Event category	Select the category of event for which the rule should apply.
Input	Select the IO module input for which the rule should apply. **Note:** For rules to be triggered by **Input Active**/**Input Normal** events, you must enable event logging on the chosen input. To do this, in ACT Manage: 1. Click **Manage > Inputs**. 2. Click the name of the input. 3. Click **Options**. 4. Select the **Log** check box. 5. Click **Save**.

6.8.2.2 Action types

Supported action types are described below.

Action	Description
Send Email	Send an email. Specify the email address for each recipient, and the text of the message. **Note:** To send emails based on rules, ensure that an email account is configured on the **Settings > SMTP** page in ACT Manage. See *Settings > SMTP Tab* on page 142.
Door Command	Issue a door command. Select the door to command, and the command to issue.
Door Output	Turn an output/relay connected to the door on/off.
Output On/Off	Turn an IO module output on/off. Select the output, and whether to turn it on or off.
Input Enabled/Disabled	Enable/disable an IO module input. Select the input, and whether to enable or disable it.

6.8.2.3 Logic operations

The rules engine supports the following logic operations:

- NOT: In this case, for the rule to evaluate as TRUE, the analyser input to the rule should evaluate as FALSE.

- AND: In this case, for the rule to evaluate as TRUE, **all** analyser inputs to the rule should evaluate as TRUE.

- OR: In this case, for the rule to evaluate as TRUE, **any** of the analyser inputs to the rule should evaluate as TRUE.

- XOR: In this case, for the rule to evaluate as TRUE, **only one** of the analyser inputs to the rule should evaluate as TRUE.

Multiple sets of analysers can be combined with multiple logic operators to feed into an action, as illustrated below.
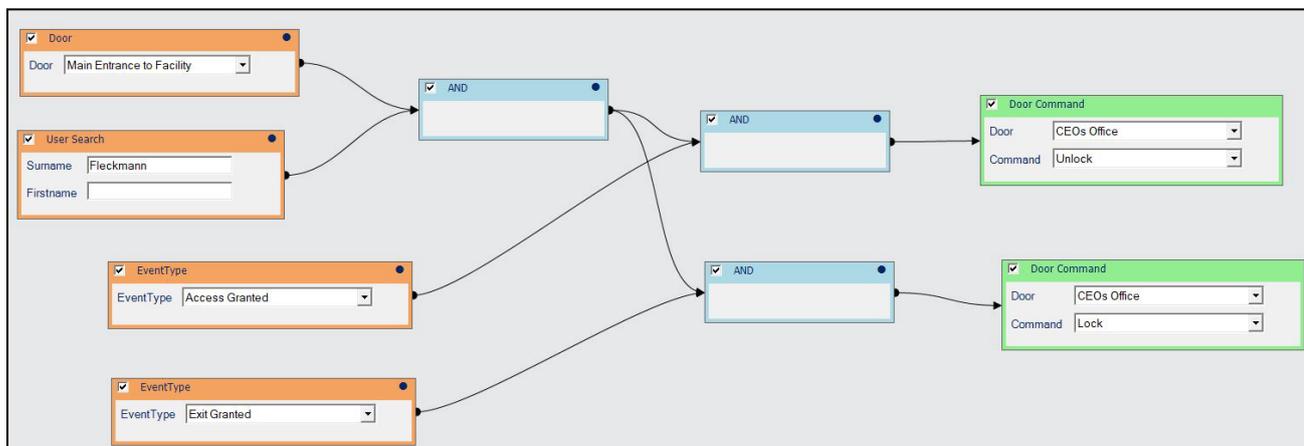
6.9 Time zones

A time zone consists of up to 8 time periods. Each period specifies a time range and the days and holidays for which the period is valid. The time zone is valid when any of its periods are valid.

Time zones are used to specify when a user/group's access rights are valid.

The following sections describe the functions available in this menu:

See also:

- *Holidays* on the facing page

- *User Group Details > Access Rights Tab* on page 99

- *User Details > Extra Rights Tab* on page 92

6.9.1 The Time Zones screen

The **Time Zones** screen shows a list of time zones configured on the system.

Field Name	Description
No	The unique number that identifies this time zone on the system. (Sortable.)
Name	The time zone's name. Click to view full details for this time zone on the **Time Zone Details** screen (see *The Time Zone Details screen* below). (Sortable.)
Active	A green clock icon indicates that the time zone is currently active. (Sortable.)
Times and Days	A summary of the times and days for which this time zone applies.

6.9.2 The Time Zone Details screen

The **Time Zone Details** screen has two tabs showing different settings for the selected time zone. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Time Zone Details > General Tab* below.
- **Tenants** tab. For more information, see *Time Zone Details > Tenants Tab* below.

6.9.3 Time Zone Details > General Tab

The following table describes the data that appears on the **Time Zone Details > General** tab.

Field Name	Description
Timezone Number	The time zone's unique identifying number on the system. This is a unique number between 1 and 255 (timezone 255 is reserved for 24 Hours access for all days). A default unique value is assigned when a new record is created. If you want to edit this value, it must be changed before the time zone record is saved for the first time.
Time zone Name	The time zone's name.
Times Days	The lower part of this tab shows a list of the Times/Days combinations when this time zone is active. To specify a Times/Days combination, select a row, and in the fields below specify the corresponding Period (From and To times), and select the Days and Holidays. The time zone is valid during any of the specified Times/Days combinations.

See also:

- *Settings > Holiday Names Tab* on page 145

6.9.4 Time Zone Details > Tenants Tab

This tab shows a list of the tenancies to which the time zone is assigned.

See also:

- *Tenancy* on page 121

6.10 Holidays

Holidays are special days during the year that can change how timezones operate.

ACT Manage allows you to specify 9 holiday types. Time zones can be configured to include days of a particular holiday type. For more information on time zones, see *Time zones* on the previous page.

For user access to be allowed on holiday days, the holiday type must be included in the time zones used when defining a user or group's access rights.

For a door action to occur on a holiday, the holiday type must be included in the time zone used when specifying the door action.

Example: A **Lock Door** action may be set up to occur on a particular holiday date. To configure this:

1. Assign the date to a holiday type. (See *The Holidays screen* below.)

2. Assign the holiday type to a timezone. (See *Time Zone Details > General Tab* on the previous page.)

3. Assign the timezone to the Lock Door action for the relevant door. (See *Door Details > Actions Tab* on page 105.)

   The door locks on this particular date.

Note: Each day can only have one assigned holiday type in ACT Enterprise.

See also:

- *Time zones* on page 110

- *User Group Details > Access Rights Tab* on page 99

- *User Details > Extra Rights Tab* on page 92

- *Door Details > Actions Tab* on page 105

6.10.1 The Holidays screen

This screen shows a 12 month calendar starting at the current month, and a list of colour-coded holiday types.

The current date is selected by default.

Dates flagged as holidays are highlighted in the corresponding holiday type colour.

To assign or change the holiday type for any date, select that date and click the **None** radio button to remove an assigned holiday type, or click the radio button for a holiday type to assign that type. Only one holiday type may be assigned to each date.

Note: Adding a holiday for a specific day/month combination leaves that holiday for that date in the system for each subsequent year. You should periodically review your holidays, for instance moving bank holidays.

See also:

- *Settings > Holiday Names Tab* on page 145

6.11 DB Users

The **DB Users** function allows you to configure operators of ACT Enterprise software, and assign them access to particular data and functions when using the software. Only ACT Enterprise administrators can view or change DB users.

The following sections describe the functions available in this menu:

6.11.1 The DB Users screen

The **DB Users** screen shows a list of operators configured on the system.

Field Name	Description
No	The unique number that identifies this operator on the system. (Sortable.)
Name	The operator's name. Click to view full details for this operator on the **DB User Details** screen (see *The DB User Details screen* below). (Sortable.)
Role	The operator's role. This determines which functions they can use and what data they can see. (Sortable.)
Windows Account	The Windows user account that is linked to this DB user.
Tenancy	The operator's tenancy. (Sortable.)

Click **Add DB User** at the top of this page to open a blank **DB User Details** screen (see *The DB User Details screen* below) from which you can add a new operator.

Select the check box for one or more operators in the list area and click **Delete DB User** at the bottom of the screen to delete the selected operator(s).

6.11.2 The DB User Details screen

The **DB User Details** screen has two tabs showing different settings for the selected operator. For more information on these tabs, click the links below.

- **General** tab. For more information, see *DB User Details > General Tab* below.
- **Tenants** tab. For more information, see *DB User Details > Tenants Tab* on the next page.

Click **Add DB User** at the bottom of this page to open a blank **DB User Details** screen from which you can add a new operator.

6.11.3 DB User Details > General Tab

The following table describes the data that appears on the **DB User Details > General** tab.

Field Name	Description
Number	The operator's unique identifying number on the system. A default unique value is assigned when a new record is created. If you want to edit this value, it must be changed before the operator record is saved for the first time.
Name	The operator's username in ACT Enterprise.
Password	For a new DB user, you can generate a password compliant with the password policy set in ACT Enterprise by clicking **Generate Password**. For an existing DB user, you can change the password by clicking **Change Password**. (See *The Change Password screen* on the next page.) In both cases, you should provide the new/changed password to the user. Passwords should comply with the password policy configured for your organisation. For more information, see *Settings > DB Users Password Policy Tab* on page 148.

Field Name	Description
Role	The role assigned to the operator. Roles are pre-defined combinations of rights to access functions and data. The **Allow** and **Database access** areas on this screen reflect the rights for the selected role. Custom indicates a combination of rights that was customised for the operator.
Use Windows Authentication	This drop-down list is populated with a list of all users on the Windows domain of the user currently logged in to ACT Install. If Windows authentication/single sign on (SSO) is supported by your organisation, select the Windows user account that should be linked to this DB user. When a user logged in to the selected Windows user account runs any ACT Enterprise client, they are automatically logged in as this DB user. **Note:** If a Windows user is associated with more than one DB user account, they are logged in to the first DB user account found by default. If this is not the correct account, the user should click **Sign out**, then log in again using the correct ACT Enterprise username and password.
Application	When you select the *Custom* role only, these selections become available. These are a convenient shortcut to allow you to assign the rights necessary for an operator to use the corresponding client. Selecting a client over-writes existing rights for the user.
Allow	Which ACT Enterprise functions the operator should have access to.
Database Access	The type of access the operator has to each data type in the ACT Enterprise database. **Full** means Read and Write access; **RO** means Read Only access; **None** means no access.

6.11.4 The Change Password screen

To change or reset an operator/DB user's password:

1. Click **Change Password** on the **DB User Details > General** tab (see *DB User Details > General Tab* on the previous page).

2. On the **Authenticate** screen, enter *your* ACT Enterprise password and click **Authenticate**.

3. On the **Change Password** screen, enter and confirm a new password for the DB user.

   Passwords should comply with the password policy configured for your organisation. For more information, see *Settings > DB Users Password Policy Tab* on page 148.

4. Click **Save**.

Provide the new password to the DB user.

6.11.5 DB User Details > Tenants Tab

This tab shows a list of the tenancies to which the operator is assigned.

See also:

- *Tenancy* on page 121

6.12 Elevator Groups

ACT Enterprise allows you to configure users to have access to different floors in an elevator lift shaft at different times.

Elevator control is one particular application of the I/O modules (IOM). The outputs on the IOM are wired into an elevator controller. Up to 32 floors may be controlled from a single ACT controller. However

controllers may be networked giving control of more floors. Outputs required for elevator control must have the Elevator Floor option assigned in the I/O module view. For more information, see *Output Details > Options Tab* on page 73.

To configure elevator access:

1. Create a Floor Group to specify all the floors available from a particular elevator. For more information, see *Elevator Manager > Floor Groups Tab* on the next page.

2. Assign the Door attached to the reader in the elevator cab to the relevant Floor Group. For more information, see *Door Details > Floor Group Tab* on page 107.

3. Create an Elevator Group, and assign all required Floor Groups and the Time zones when access to those Floor Groups is allowed. For more information, see *Elevator Manager > Elevator Groups Tab* below.

4. Assign the Elevator Group to a User Group. Any user assigned to the User Group is allowed access to the Floor Groups assigned to the Elevator Group during the specified Time zones. For more information, see *User Group Details > General Tab* on page 98.

The following sections describe the functions available in this menu:

6.12.1 The Elevator Manager screen

The **Elevator Manager** screen has two tabs showing Elevator Groups and Floor Groups. For more information on these tabs, click the links below.

- **Elevator Groups** tab. For more information, see *Elevator Manager > Elevator Groups Tab* below.

- **Floor Groups** tab. For more information, see *Elevator Manager > Floor Groups Tab* on the next page.

6.12.2 Elevator Manager > Elevator Groups Tab

The **Elevator Groups** tab shows a list of elevator groups configured on the system.

Field Name	Description
No	The unique number that identifies this elevator group on the system. (Sortable.)
Name	The elevator group's name. Click to view full details for this elevator group on the **Elevator Group Details** screen (see *The Elevator Group Details screen* on the next page). (Sortable.)

6.12.3 The Elevator Group Details screen

The **Elevator Group Details** screen has two tabs. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Elevator Group Details > General Tab* below.
- **Tenants** tab. For more information, see *Elevator Group Details > Tenants Tab* below.

6.12.4 Elevator Group Details > General Tab

The following table describes the data that appears on the **Elevator Group Details > General** tab.

Field Name	Description
Number	The elevator group's unique identifying number on the system.
Name	The elevator group's name.
Floor Group/ Time Zone combinations	The list of floor groups that may be accessed by users assigned to this elevator group, and the corresponding time zones during which access is granted. Up to 8 combinations can be configured. To assign a new floor group/time zone combination, select an empty row here, then select the required values from the **Floor Groups** and **Time zones** drop-down lists at the bottom of the screen and click **Assign**. To remove a floor group/time zone combination, select the row for that combination here, then click **Unassign**.

6.12.5 Elevator Group Details > Tenants Tab

This tab shows a list of the tenancies to which the elevator group is assigned.

See also:

- *Tenancy* on page 121

6.12.6 Elevator Manager > Floor Groups Tab

The **Floor Groups** tab shows a list of floor groups configured on the system.

Field Name	Description
No	The unique number that identifies this floor group on the system. (Sortable.)
Name	The floor group's name. Click to view full details for this floor group on the **Floor Group Details** screen (see *The Floor Group Details screen* below). (Sortable.)

6.12.7 The Floor Group Details screen

The **Floor Group Details** screen has two tabs. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Floor Group Details > General Tab* below.
- **Tenants** tab. For more information, see *Floor Group Details > Tenants Tab* on the facing page.

6.12.8 Floor Group Details > General Tab

The following table describes the data that appears on the **Floor Group Details > General** tab.

Field Name	Description
Number	The floor group's unique identifying number on the system.

Field Name	Description
Name	The floor group's name.
Controller	The controller associated with this floor group.
Available Floors	This list shows all floors available. To add a floor to the **Assigned Floors** list, select the floor here, then click the right-arrow (▶). To add all floors, click the double-right-arrow (▶▶).
Assigned Floors	This list shows all assigned floors in the Floor Group. To remove a floor from the list, select it in the **Assigned Floors** list and click the left-arrow (◀). To remove all floors, click the double-left-arrow (◀◀).

6.12.9 Floor Group Details > Tenants Tab

This tab shows a list of the tenancies to which the floor group is assigned.

See also:

- *Tenancy* on page 121

6.13 Inputs and Outputs

The I/O (Input/Output) Module (IOM) is an 8 Input/8 Output device that allows ACT controllers to receive/send signals from/to other electronic equipment. For example, an IOM could be connected to elevator controls, alarm systems or CCTV switching.

A maximum of 4 IOMs can be connected to any single ACT controller, giving control of up to 32 inputs and 32 outputs (relays) per controller (4 times 8).

ACT Manage allows you to configure settings for IOMs on the physical network.

The following sections describe the functions available in this menu:

6.13.1 The Inputs screen

The **Inputs** screen shows a list of inputs on the system.

Field Name	Description
No	The unique number that identifies this input on the system. (Sortable.)
Name	The input's name. Click to view full details for this input on the **Input Details** screen (see *The Input Details screen* below). (Sortable.)
Status	The input's status: **Online** or **Offline**. (Sortable.)

6.13.2 The Input Details screen

The **Input Details** screen has a number of tabs showing different settings for the selected input. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Input Details > General Tab* below.
- **Enable** tab. For more information, see *Input Details > Enable Tab* below.
- **Activate** tab. For more information, see *Input Details > Activate Tab* below.
- **Options** tab. For more information, see *Input Details > Options Tab* on the facing page.
- **Tenants** tab. For more information, see *Input Details > Tenants Tab* on the facing page.

6.13.3 Input Details > General Tab

The following table describes the data that appears on the **Input Details > General** tab.

Field Name	Description
Input Name	The input's name. This name appears in the log when the input changes state.
Timer	The amount of time in seconds that the input must remain in a certain state before the change is reported. This prevents a momentary change in the input from causing a false alarm.
Controller	The controller to which the input is connected.

6.13.4 Input Details > Enable Tab

The following table describes the data that appears on the **Input Details > Enable** tab.

Field Name	Description
Timezone	The time zone during which this relay is active. If the input is unused, this should be set to **No Time Zone**.
Output	Inputs can be configured to be dependent on active outputs. When the specified output is active, this input is also active.

6.13.5 Input Details > Activate Tab

The following table describes the data that appears on the **Input Details > Activate** tab.

Field Name	Description
Output	An output may be programmed to follow the state of an input or a door. If an output is selected here, then as the input activates, the selected output also activates. When the input deactivates, the output de-activates.

Field Name	Description
Door	A door may be programmed to follow the state of an input. If a door is selected on this tab, then as the input activates, the selected door also activates. When the input deactivates, the door de-activates.

6.13.6 Input Details > Options Tab

The following table describes the data that appears on the **Input Details > Options** tab.

Field Name	Description
Normally Open	If selected, the input is in the normal state when the contact is open and active when the contact is closed.
Supervised	If selected, the IOM checks for tampers and shorts across the input contacts.
Log	If selected, the input is logged while enabled.
Alarm	If selected, an alarm is triggered when this input becomes active.

6.13.7 Input Details > Tenants Tab

This tab shows a list of the tenancies to which the input is assigned.

See also:

- *Tenancy* on page 121

6.13.8 The Outputs screen

The **Outputs** screen shows a list of outputs on the system.

Field Name	Description
No	The unique number that identifies this output on the system. (Sortable.)
Name	The output's name. Click to view full details for this input on the **Output Details** screen (see *The Output Details screen* below). (Sortable.)
Status	The output's status: **Online** or **Offline**. (Sortable.)

6.13.9 The Output Details screen

The **Output Details** screen has a number of tabs showing different settings for the selected output. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Output Details > General Tab* on the next page.

- **Options** tab. For more information, see *Output Details > Options Tab* on the next page.

- **Follow Door** tab. For more information, see *Output Details > Follow Door Tab* on the next page.

- **Output On Event** tab. For more information, see *Output Details > Output On Event Tab* on the next page.

- **Output Off Event** tab. For more information, see *Output Details > Output Off Event Tab* on page 121.

- **Tenants** tab. For more information, see *Output Details > Tenants Tab* on page 121.

6.13.10 Output Details > General Tab

The following table describes the data that appears on the **Output Details > General** tab.

Field Name	Description
Output Name	The output's name.
Timer	The amount of time in seconds that the output must remain in a certain state before the change is reported. This prevents a momentary change in the output from causing a false alarm.
Active Timezone	The time zone during which this relay is active.
Controller	The controller to which the input is connected.

See also:

- *Time zones* on page 110

6.13.11 Output Details > Options Tab

The following table describes the data that appears on the **Output Details > Options** tab.

Field Name	Description
Log	If selected, the output is logged while enabled.
Normally On	If selected, the output is in the normal state when the contact is open and active when the contact is closed.
Elevator Floor	If selected, the output may be used for elevator control.

See also:

- *Elevator Groups* on page 114

6.13.12 Output Details > Follow Door Tab

An output may be programmed to follow the state of an input or a door on the same controller.

If a door is selected on this tab, then as that door opens, the output activates. When the door closes, the output de-activates.

6.13.13 Output Details > Output On Event Tab

The following table describes the data that appears on the **Output Details > Output On Event** tab.

When the event described by the conditions set on this tab occurs, the output relay is turned on.

Field Name	Description
Event	The event type that triggers turning the output on.
Door	The door at which the event occurs.
Area	The area in which the event occurs.
User Group	The user group for which the event occurs.

6.13.14 Output Details > Output Off Event Tab

The following table describes the data that appears on the **Output Details > Output Off Event** tab.

When the event described by the conditions set on this tab occurs, the output relay is turned off.

Field Name	Description
Event	The event type that triggers turning the output off.
Door	The door at which the event occurs.

6.13.15 Output Details > Tenants Tab

This tab shows a list of the tenancies to which the output is assigned.

See also:

- *Tenancy* below

6.14 Tenancy

Multi-tenancy allows large systems, with a large number of doors and users, to be broken down into smaller, more manageable systems (sites/tenancies).

Multi-tenancy is also used to allow multiple companies/organisations to share the same physical access control system but manage their own users and doors. For example, in large office blocks shared by many smaller companies, if the landlord installed one access control system for the building, each individual company can be assigned a tenancy and allowed to operate its own access control system.

Note: Multi-tenancy is an add-on package to the basic ACT Enterprise suite and must be purchased separately.

ACT Enterprise operators (database users) must be created for each tenant on the system, and components (users, door, etc.) assigned to the appropriate tenancy. Operators can only view and configure users and settings relevant to their site. They cannot see activity on other sites.

Note: Administrator users can see all activity across all tenancies.

The following sections describe the functions available in this menu:

6.14.1 The Sites screen

The following table describes the search field and results columns on the **Sites** screen.

Field Name	Description
Search	Enter all or part of the name of the site you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area.
No	The unique number that identifies this site on the system. (Sortable.)
Name	The site's name. Click to view full details for this user on the **Site Details** screen (see *The Site Details screen* below). (Sortable.)

6.14.2 The Site Details screen

The **Site Details** screen has a number of tabs showing different settings for the selected site. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Site Details > General Tab* below.
- **DB Users** tab. For more information, see *Site Details > DB Users Tab* below.
- **Users** tab. For more information, see *Site Details > Users Tab* on the facing page.
- **User Groups** tab. For more information, see *Site Details > User Groups Tab* on the facing page.
- **Controllers** tab. For more information, see *Site Details > Controllers Tab* on page 124.
- **Doors** tab. For more information, see *Site Details > Doors Tab* on page 124.
- **Door Groups** tab. For more information, see *Site Details > Door Groups Tab* on page 125.
- **Elevator Groups** tab. For more information, see *Site Details > Elevator Groups Tab* on page 125.
- **Floor Groups** tab. For more information, see *Site Details > Floor Groups Tab* on page 125.
- **I/O Modules** tab. For more information, see *Site Details > I/O Modules Tab* on page 126.
- **Time Zones** tab. For more information, see *Site Details > Time Zones Tab* on page 126.

6.14.3 Site Details > General Tab

The following table describes the data that appears on the **Site Details > General** tab.

Field Name	Description
Site Number	The site's unique identifying number on the system.
Site Name	The site's name.

6.14.4 Site Details > DB Users Tab

This tab shows a list of DB Users (operators) with access to this tenancy/site. DB Users can also be assigned access to tenancies on the **DB User Details > Tenants** tab (see *DB User Details > Tenants Tab* on page 114).

The following table describes the fields on the **Site Details > DB Users** screen.

Field Name	Description
Filter by	Filter the list of DB Users by selecting whether to **Show All**, **Assigned** or **Unassigned** operators.
	If you know all or part of the DB User's name, enter that in the **Name** field.
	The list of DB Users below updates to match your filter.
Name	The name of the DB User. Click to view their details on the **DB User Details** screen (see *The DB User Details screen* on page 113).
Role	The role assigned to the DB User on the **DB User Details** screen (see *The DB User Details screen* on page 113). Their role determines which functions and data they have access to in ACT Enterprise.
Assigned	Whether the DB User is assigned to the current site.
	To assign a DB User to the current site, select the button to the left of their name and click **Assign**, then **Save**.
	To unassign a DB User from the current site, select the button to the left of their name and click **Unassign**, then **Save**.

6.14.5 Site Details > Users Tab

This tab shows a list of Users assigned to this tenancy/site. Users can also be assigned to tenancies on the **User Details > Tenants** tab (see *User Details > Tenants Tab* on page 94).

The following table describes the fields on the **Site Details > Users** screen.

Field Name	Description
Filter by	Filter the list of users by selecting whether to **Show All**, **Assigned** or **Unassigned** users.
	If you know all or part of the user's name, enter that in the **Name** field.
	The list of users below updates to match your filter.
User	The name of the user. Click to view their details on the **User Details** screen (see *The User Details screen* on page 89).
Group	The group the user belongs to. Click to view the group details on the **Group Details** screen (see *User Group Details Screen* on page 98).
Assigned	Whether the user is assigned to the current site.
	To assign a user to the current site, select the button to the left of their name and click **Assign**, then **Save**.
	To unassign a user from the current site, select the button to the left of their name and click **Unassign**, then **Save**.

6.14.6 Site Details > User Groups Tab

This tab shows a list of User Groups assigned to this tenancy/site. Users can also be assigned to tenancies on the **User Group Details > Tenants** tab (see *User Group Details > Tenants Tab* on page 101).

The following table describes the fields on the **Site Details > User Groups** screen.

Field Name	Description
Filter by	If you know all or part of the User Group's name, enter that in the **Name** field. The list of User Groups below updates to match your filter.
Available	This list shows all user groups available. To add a user group to the **Assigned** list, select the user group here, then click the right-arrow (▶). To add access to all user groups, click the double-right-arrow (▶▶).
Assigned	This list shows all user groups assigned to the current site. To remove a user group, select it here and click the left-arrow (◀). To remove all user groups, click the double-left-arrow (◀◀).

6.14.7 Site Details > Controllers Tab

This tab shows a list of Controllers assigned to this tenancy/site.

The following table describes the fields on the **Site Details > Controllers** screen.

Field Name	Description
Filter by	If you know all or part of the Controller's name, enter that in the **Name** field. The list of Controllers below updates to match your filter.
Available	This list shows all controllers available. To add a controller to the **Assigned** list, select it here, then click the right-arrow (▶). To add access to all controllers, click the double-right-arrow (▶▶).
Assigned	This list shows all controllers assigned to the current site. To remove a controller, select it here and click the left-arrow (◀). To remove all controllers, click the double-left-arrow (◀◀).

6.14.8 Site Details > Doors Tab

This tab shows a list of Doors assigned to this tenancy/site. Doors can also be assigned to tenancies on the **Door Details > Tenants** tab (see *Door Details > Tenants Tab* on page 107).

The following table describes the fields on the **Site Details > Doors** screen.

Field Name	Description
Filter by	If you know all or part of the Door's name, enter that in the **Name** field. If you know the Door Group the Door belongs to, select that from the **Group** drop-down list. The list of Doors below updates to match your filter.
Available	This list shows all doors available. To add a door to the **Assigned** list, select it here, then click the right-arrow (▶). To add access to all doors, click the double-right-arrow (▶▶).

Field Name	Description
Assigned	This list shows all doors assigned to the current site.
	To remove a door, select it here and click the left-arrow (◀).
	To remove all doors, click the double-left-arrow (◀◀).

6.14.9 Site Details > Door Groups Tab

This tab shows a list of Door Groups assigned to this tenancy/site. Door Groups can also be assigned to tenancies on the **Door Group Details > Tenants** tab (see *Door Group Details > Tenants Tab* on page 103).

The following table describes the fields on the **Site Details > Door Groups** screen.

Field Name	Description
Filter by	If you know all or part of the Door Group's name, enter that in the **Group Name** field.
	The list of Door Groups below updates to match your filter.
Available	This list shows all door groups available.
	To add a door group to the **Assigned** list, select it here, then click the right-arrow (▶).
	To add access to all door groups, click the double-right-arrow (▶▶).
Assigned	This list shows all door groups assigned to the current site.
	To remove a door group, select it here and click the left-arrow (◀).
	To remove all door groups, click the double-left-arrow (◀◀).

6.14.10 Site Details > Elevator Groups Tab

This tab shows a list of Elevator Groups assigned to this tenancy/site. Elevator Groups can also be assigned to tenancies on the **Elevator Group Details > Tenants** tab (see *Elevator Group Details > Tenants Tab* on page 116).

The following table describes the fields on the **Site Details > Elevator Groups** screen.

Field Name	Description
Filter by	If you know all or part of the Elevator Group's name, enter that in the **Name** field.
	The list of Elevator Groups below updates to match your filter.
Available	This list shows all elevator groups available.
	To add an elevator group to the **Assigned** list, select it here, then click the right-arrow (▶).
	To add access to all elevator groups, click the double-right-arrow (▶▶).
Assigned	This list shows all elevator groups assigned to the current site.
	To remove an elevator group, select it here and click the left-arrow (◀).
	To remove all elevator groups, click the double-left-arrow (◀◀).

6.14.11 Site Details > Floor Groups Tab

This tab shows a list of Floor Groups assigned to this tenancy/site. Floor Groups can also be assigned to tenancies on the **Floor Group Details > Tenants** tab (see *Floor Group Details > Tenants Tab* on page 117).

The following table describes the fields on the **Site Details > Floor Groups** screen.

Field Name	Description
Filter by	If you know all or part of the Floor Group's name, enter that in the **Name** field. The list of Floor Groups below updates to match your filter.
Available	This list shows all floor groups available. To add a floor group to the **Assigned** list, select it here, then click the right-arrow (▶). To add access to all floor groups, click the double-right-arrow (▶▶).
Assigned	This list shows all floor groups assigned to the current site. To remove a floor group, select it here and click the left-arrow (◀). To remove all floor groups, click the double-left-arrow (◀◀).

6.14.12 Site Details > I/O Modules Tab

This tab shows a list of I/O Modules assigned to this tenancy/site. I/O Modules can also be assigned to tenancies on the **Input Details > Tenants** tab (see *Input Details > Tenants Tab* on page 119) and the **Output Details > Tenants** tab (see *Output Details > Tenants Tab* on page 121).

The following table describes the fields on the **Site Details > I/O Modules** screen.

Field Name	Description
Filter by	If you know all or part of the I/O Module's name, enter that in the **Name** field. If you know which controller the I/O Module is connected to, select that from the **Controller Name** drop-down list. The list of I/O Modules below updates to match your filter.
Available	This list shows all I/O Modules available. To add an I/O Module to the **Assigned** list, select it here, then click the right-arrow (▶). To add access to all I/O Modules, click the double-right-arrow (▶▶).
Assigned	This list shows all I/O Modules assigned to the current site. To remove an I/O Module, select it here and click the left-arrow (◀). To remove all I/O Modules, click the double-left-arrow (◀◀).

6.14.13 Site Details > Time Zones Tab

This tab shows a list of Time Zones assigned to this tenancy/site. Time Zones can also be assigned to tenancies on the **Time Zone Details > Tenants** tab (see *Time Zone Details > Tenants Tab* on page 111).

The following table describes the fields on the **Site Details > Time Zones** screen.

Field Name	Description
Filter by	If you know all or part of the Time Zone's name, enter that in the **Name** field. The list of Time Zones below updates to match your filter.

Field Name	Description
Available	This list shows all Time Zones available. To add a Time Zone to the **Assigned** list, select it here, then click the right-arrow (▶). To add access to all Time Zones, click the double-right-arrow (▶▶).
Assigned	This list shows all Time Zones assigned to the current site. To remove a Time Zone, select it here and click the left-arrow (◀). To remove all Time Zones, click the double-left-arrow (◀◀).

6.15 Cards

Cards are physical items presented to door readers by users in order to authenticate themselves and gain access according to their access rights.

Note: The **Card Editor** option on this menu launches the Card Editor which allows you to design the appearance of cards.

The following sections describe the functions available in this menu:

See also:

- *User Group Details > Default Card Tab* on page 100

6.15.1 The Extra Cards screen

Note: Extra cards can only be assigned on systems that explicitly allow this. You must have controllers capable of storing additional cards and the **Allow multiple cards per user** option must be enabled on the **Card Configuration** screen in ACT Install (see *Card Configuration* on page 73).

The following table describes the fields that appear on the **Extra Cards** screen.

Field Name	Description
Card Type	Select the type of card you want to add.
First Card	To create a range of extra cards, enter the number of the first card here.
Last Card	To create a range of extra cards, enter the number of the last card here.
First User	Click **Find User** to find the first available user number from which a sufficiently long sequence of free user numbers exists to assign the extra cards sequentially.
Default User Group	To set the default user group of users created during this operation, select the user group here.

Click **Add Cards** to create a list of users and assigned cards according to your settings.

A summary screen shows a list of users to be created based on your settings. You can modify the first name, last name, group and enabled status for each user here before clicking **Save** to create them on the system.

Note: The users are **not** created on the system **until** you click **Save** on the results screen.

6.15.2 The Report Lost screen

This screen allows you to disable, or reset the validity for, a user's cards if they report them as lost/stolen.

The following table describes the search fields available on the **Report Lost** screen.

Field Name	Description
Search	Enter all or part of the registered name for the user whose cards you want to view and click the **Search** icon (🔎). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**anne** Murphy", and "Joseph H**ann**".
Advanced. Click **Advanced** to see the following additional search fields.	
By Card Number	Select this option to search for a record using the number of the user's card. Enter the card number in the corresponding field and press **Return**. Only cards that match the number exactly are returned in the search results.
By User	Select this option to search for a record using details of the user who owns the card. Enter all or part of the user's **First Name**, **Last Name**, or **User Number**, then press **Return**. Partial matches are returned for first name and last name, as with the default **Search** field. If you specify a user number, only the user that matches the number exactly is returned in the search results.

The following table describes each of the columns on the **Report Lost** screen search results area.

Column Name	Description
No	The unique number that identifies this user on the system. (Sortable.)
User	The user's name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on page 89). (Sortable.)
Enabled	A green check-mark is displayed for accounts that are enabled. If an account is enabled, the user's card/PIN is operative, though usage may be restricted by a validity period, if set. If an account is disabled, the user's card/PIN does not work. An account must be both enabled **and** valid for the user's card/PIN to work.
Expiration	When the user's account is set to expire.
OneToOne	The number of the user's One-To-One card, if they have one.
SiteCoded	The number of the user's Site Coded card, if they have one. **Note:** Site code support is a legacy feature in ACT Enterprise and cannot be enabled or configured in new installations.
Card 3	The number of the user's third card, if they have one.
Card 4	The number of the user's fourth card, if they have one.
Card 5	The number of the user's fifth card, if they have one.

6.16 Tools (ACT Manage)

This section describes the tools available in ACT Manage:

6.16.1 System Synchronise

The System Synchronise Wizard allows you to download the entire database to one or more controllers. Synchronising controllers means that all data entered on the controller directly, via its keypad, is lost. Controllers remain offline during downloads, meaning that they cannot be commanded during this time, nor can they report events. Door stations have limited functionality during the download. You should only do a download if you are certain it is required.

Follow the on-screen instructions, clicking **Next** between steps and **Finish** at the end.

- **Step 1: Controllers.** This screen indicates whether each controller is up to date or not. Select which controllers you want to download to.

- **Step 2: Downloading.** The progress bar shows the overall progress of the system synchronisation. The message area shows information for each controller.

- **Step 3: Results.** The results of the synchronisation operation are shown: the number of controllers updated and their current statuses.

6.16.2 Reset

The **Reset** screen allows you to reset muster, anti-passback and counting areas.

6.16.3 Populate notes, email, or mobile

The **Populate notes, email, or mobile** tool facilitates data migration from custom user data fields (on the **User Details > Details** tab) to standard fields on the **User Details > General** tab. Supported destination fields are **Email**, **Mobile**, and **Notes**.

When this tool copies data to the **User Details > General** tab, it overwrites any existing information in the destination field.

If the source field on the **User Details > Details** tab is empty *for all users*, the tool displays a warning and does not migrate data, but if the source field on the **User Details > Details** tab is empty for a subset of users only, the "empty" value is copied to the destination field for those users, and any value already specified on the **User Details > General** tab is deleted.

Because of the potential to overwrite/delete data, Vanderbilt recommend that you back up your database before using this tool. See *Backups* on page 49.

To use the tool:

1. In ACT Manage, click **Tools > Populate notes, email, or mobile**.

2. From the **Field to Populate** drop-down list, select the name of the field on the **User Details > General** tab to which you want to copy data.

3. From the **Copy From** drop-down list, select the name of the field on the **User Details > Details** tab from which you want to copy data.

4. To delete data from the **User Details > Details** tab after it has been copied to the **User Details > General** tab, select the **Blank user field after copy?** check-box.

5. Click **Copy**.

   A popup displays a message confirming whether the data migration operation was successful.

6.17 Reports (ACT Manage)

ACT Manage allows you to generate a number of reports on ACT Enterprise data according to specific criteria. This section describes the report types available.

> **i** If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.

6.17.1 Validate Users report

The **Validate Users** report is accessed through the **Reports > Validate Users** menu item in ACT Manage.

The **Validate Users** screen allows you to:

- Search for users whose validity period has expired, or expires soon.

- Search for inactive users, whose cards have not been recently used. Inactive users may have lost their cards, or no longer be in the relevant company or organisation.

Once you have identified the user(s) of interest, select one or more users and click the relevant button at the bottom of the screen to delete, enable or disable their accounts, or to edit their validity period (see *Change Validity* on the facing page).

See also:

- *Search Fields* below

- *Results* on the facing page

6.17.1.1 Search Fields

Field Name	Description
Search	Enter all or part of the registered name for the user whose record you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**anne** Murphy", and "Joseph H**ann**".
Advanced. Click **Advanced** to see the following additional search fields. Specify criteria and click **Search**. To report on users with expired/expiring validity, use the **Expired**, **Expire By** and **Expire By** date fields. To report on inactive users, use the *Inactive* field.	
User Group	Select the group to which the user is assigned.

Field Name	Description
Expired	Select to view users who have already expired, that is, their validity period has ended.
Inactive	Select to view users who have been inactive for a period of time, and select the required time period from the corresponding drop-down list. **Note:** If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.
Expire By	Select to view users who are due to expire in a certain timeframe, and select whether that timeframe is **Today**, **Next Week** or **Next Month** from the corresponding drop-down list.
All Users	Select to view all users.
Expire By Date	Select to view users who are due to expire by a certain date, and specify that date.

6.17.1.2 Results

The following table describes each of the columns on the **Validate Users** screen search results area.

Column Name	Description
No.	The unique number that identifies this user on the system. (Sortable.)
Name	The user's name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on page 89). (Sortable.)
Group	The group this user is a member of. Click to view full details for this group on the **Group Details** screen (see *User Group Details Screen* on page 98). (Sortable.)
Enabled	A green check-mark is displayed for accounts that are enabled.
Valid From	When the user is valid from.
Valid To	When the user is valid until.
Valid	A green check-mark is displayed for accounts that are valid. A user's account is valid if either the current date and time fall within the set validity period, or if no validity period was set for the user.
Last activity	The last date and time activity was recorded for the user. **Note:** If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.

6.17.2 Change Validity

Set **From** and **To** dates and times then click **Save** to change the validity period for the users listed at the bottom of this screen.

6.17.3 User List report

The **User List** report is accessed through the **Reports > User List** menu item in ACT Manage.

See also:

- *Search Fields* on the next page
- *Results* on the next page

6.17.3.1 Search Fields

Field Name	Description
Simple Tab Filter	
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all users. • **Users With Access to Door** – select a particular door. • **Belonging to Group** – select a particular user group.
Advanced Tab Filter	
Only Enabled Users	Select to report on enabled users only.
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all users. • **Users With Access to Door** – select a particular door. • **Belonging to Group** – select a particular user group. • **Range** – specify a range of user numbers to report on. • **User Details** – select any user details field type to search on and specify all or part of the required value for that field.
Show	Select whether to show the user's photo in the first column of the search results, and what information to show in the last two columns of the search results.

Click **Generate** to generate a report according to your search criteria.

6.17.3.2 Results

The following table describes each of the columns on the **User List** screen search results area.

Column Name	Description
Photo	This column only appears if **Show photo** is selected in the **Advanced** search criteria. It shows a small version of the user's photo.
No.	The unique number that identifies this user on the system. (Sortable.)
User	The user's name. (Sortable.) Click a user's name to view the user's profile on the **User Details** screen (see *The User Details screen* on page 89). Click the **Back** icon (◀) at the top of the **User Details** screen to return to the **Users** screen.
Enabled	A green check-mark is displayed for accounts that are enabled.
Group	The group this user is a member of. Click to view full details for this group on the **Group Details** screen (see *User Group Details Screen* on page 98). (Sortable.)
Card number	The user's card number. You can change which card number is shown using the **Advanced** search settings.

Column Name	Description
Last column	The default value displayed in the last column is determined by the Optional Column setting on the **Settings > General** tab (see *Settings > General Tab* on page 140), but you can change which user field value is shown using the **Advanced** search settings.

6.17.4 Card Expiry report

The **Card Expiry** report is accessed through the **Reports > Card Expiry** menu item in ACT Manage.

See also:

- *Search Fields* below

- *Results* on the next page

6.17.4.1 Search Fields

Field Name	Description
Simple Tab Filter	
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all users. • **Users With Access to Door** – select a particular door. • **Belonging to Group** – select a particular user group.
Expiry In	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **1 Week** – select to view accounts expiring in the next week. • **Number of Days** – specify a number of days. • **On Date** – specify a particular date.
Options	Select whether to **Include Expired Cards** in the report.
Advanced Tab Filter	
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all users. • **Users With Access to Door** – select a particular door. • **Belonging to Group** – select a particular user group. • **Range** – specify a range of user numbers to report on.

Field Name	Description
Expiry In	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **1 Week** – select to view accounts expiring in the next week. • **2 Weeks** – select to view accounts expiring in the next 2 week. • **3 Weeks** – select to view accounts expiring in the next 3 week. • **4 Weeks** – select to view accounts expiring in the next 4 week. • **Number of Days** – specify a number of days. • **On Date** – specify a particular date.
Options	Select whether to **Include Expired Cards** in the report.

Click **Generate** to generate a report according to your search criteria.

6.17.4.2 Results

The following table describes each of the columns on the **Card Expiry** screen search results area.

Column Name	Description
No.	The unique number that identifies this user on the system. (Sortable.)
User	The user's name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on page 89). (Sortable.)
Enabled	A green check-mark is displayed for accounts that are enabled. (Sortable.)
Group	The group this user is a member of. Click to view full details for this group on the **Group Details** screen (see *User Group Details Screen* on page 98). (Sortable.)
Valid From	The date the user's account is valid from. (Sortable.)
Expiry Date	The date the user's account expires. (Sortable.)
Expired	Whether the user's account is expired. (Sortable.)

6.17.5 User Tracking report

The **User Tracking** report is accessed through the **Reports > User Tracking** menu item in ACT Manage.

See also:

- *Search Fields* below
- *Results* on the facing page

6.17.5.1 Search Fields

Field Name	Description
Simple Tab Filter	
Report	Select whether to generate a **Muster** report (all users currently on site), or an **Absentee List** report (users not on site).

Field Name	Description
Time	Select whether to generate the report for **Today** or a **Custom** time period.
	Note: If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.
Advanced Tab Filter	
Report	Select the report type to generate.
Doors	Select a door type or group to report on.
Users	Select whether to report on all users, users in a particular group, or users with **Monitor User** set on the **User Details > Options** tab (see *User Details > Options Tab* on page 91).
Options	Select whether to show the user's photo in the first column of the search results, whether to report on enabled users only, and what information to show in the last column of the search results for all reports except the **Absentee List**.
Time	Specify the time period to report for.
	Note: If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.

Click **Generate** to generate a report according to your search criteria.

6.17.5.2 Results

The following table describes each of the columns on the **User Tracking** screen search results area.

Note: Results on the current results page only may be sorted.

Column Name	Description
Photo	This column only appears if **Show photo** is selected in the **Advanced** search criteria. It shows a small version of the user's photo.
Time	The event time.
Event	The event type.
Location	The event location.
User Name	The user's name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on page 89).
Last Column	This column appears for all reports except for **Absentee List**.
	The default value displayed in the last column is determined by the **Optional Column** setting on the **Settings > General** tab (see *Settings > General Tab* on page 140), but you can change which user field value is shown using the **Advanced** search settings.

6.17.6 Audit Trail report

The **Audit Trail** report is accessed through the **Reports > Audit Trail** menu item in ACT Manage.

See also:

- *Search Fields* on the next page
- *Results* on the next page

6.17.6.1 Search Fields

Field Name	Description
Time	Select whether to generate the report for **Today, This Week, This Month** or a **Custom** time period.
Select database user	Select the database user (operator) to report on.
Show audit trail events	Select which events to include in the report.

Click **Generate** to generate a report according to your search criteria.

6.17.6.2 Results

The following table describes each of the columns on the **Audit Trail** screen search results area.

Note: Results on the current results page only may be sorted.

Column Name	Description
Time	The event time.
User	The Operator name. Click to view full details for this operator on the **DB User Details** screen (see *The DB User Details screen* on page 113).
Event	The event type.
Details	Details related to the event, for example the particular record edited if the event was **Record modified**.
User or record name	The name of the record modified.

6.17.7 Event Analysis report

The **Event Analysis** report is accessed through the **Reports > Event Analysis** menu item in ACT Manage.

See also:

- *Search Fields* below
- *Results* on the facing page

6.17.7.1 Search Fields

Field Name	Description
Simple Tab Filter	
Users	Select **All** to report on all users, or **Single** to open the **User Lookup** screen (see *The User Lookup screen* on page 14) where you can select a particular user to report on.
Time	Select whether to generate the report for **Today,** a particular time (**Spot Check**) or a **Custom** time period. A **Spot Check** report includes a time period either side of the specified time – this is specified by the **Spot interval** value on the **Settings > General** tab (see *Settings > General Tab* on page 140).
	Note: If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.

Field Name	Description
Advanced Tab Filter	
Events	Select the event types to include in the report.
Users	Select **All** to report on all users, users **Belonging to User Group** to report on users in a selected User Group only, or **Single** to open the **User Lookup** screen where you can select a particular user to report on (see *The User Lookup screen* on page 14).
Doors	Select **All** to report on all doors, **Single** to report on one particular door, or **Belonging to Door Group** to report on all doors in a particular door group.
Time	Select whether to generate the report for **Today,This Week**, **This Month**, a particular time (**Spot Check**) or a **Custom** time period. A **Spot Check** report includes a time period either side of the specified time – this is specified by the **Spot interval** value on the **Settings > General** tab (see *Settings > General Tab* on page 140).
	Note: If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.

Click **Generate** to generate a report according to your search criteria.

6.17.7.2 Results

The following table describes each of the columns on the **User Tracking** screen search results area.

Column Name	Description
Time	The event time. (Sortable.)
Event	The event type. (Sortable.)
Location	The event location. (Sortable.)
Details	Details for the event. (Sortable.)

6.17.8 Time and Attendance report

The **Time and Attendance** report is accessed through the **Reports > Time and Attendance** menu item in ACT Manage.

> This is a basic T&A report, based on events at entry and exit doors in the system. It is also possible to integrate ACT Enterprise with a third party T&A system. For more information on T&A options in ACT Enterprise, see *Report on time and attendance (T&A)* on page 45.

See also:

- *Search Fields* below
- *Results* on the next page

6.17.8.1 Search Fields

Field Name	Description
Users	Select **All** to report on all users, users **Belonging to User Group** to report on users in a selected User Group only, or **Single** to open the **User Lookup** screen where you can select a particular user to report on (see *The User Lookup screen* on page 14).

Field Name	Description
Doors	Select **All** to report on all doors, **Single** to report on one particular door, or **Belonging to Door Group** to report on all doors in a particular door group.
Time	Select whether to generate the report for **Today, This Week**, **This Month**, a particular time (**Spot Check**) or a **Custom** time period. A **Spot Check** report includes a time period either side of the specified time – this is specified by the **Spot interval** value on the **Settings > General** tab (see *Settings > General Tab* on page 140). **Note:** If ACT Enterprise is configured to delete log events for a user when they are deleted, or to auto purge log events after a period of time, this impacts what data is available for reporting on user activity.
Totals	Select whether the **Total Time** column should display: • Total For Normal Hours – The total number of normal hours worked by the user. • Total For Overtime Hours – The total number of overtime hours worked by the user. • Total For All Hours – The total number of hours worked across normal and overtime hours by the user. The normal and overtime hours for a user are determined by the user group to which the user belongs. For more information on configuring normal and overtime hours, see *User Group Details > T&A Report Tab* on page 101. Totals are calculated by summing the figures in the **Time** column for the user.
Report Options	Optionally, select the check box for each applicable reporting option: • **Join Unpaired Events** – If this check box is selected, then if user logins/logouts are missing in the event log, ACT Enterprise joins unpaired events for reporting purposes. For example, if the event log shows a user logging in at 08:00, logging in again at 12:30, and logging out at 16:30, ACT Enterprise joins the unpaired 08:00 login event to the 12:30 login event, resulting in a total period of 08:00–16:30. • **Restrict To Max Hours Per Day** – If this check box is selected, then if a user works in excess of the configured maximum number of hours for users in their user group, ACT Enterprise reports the configured maximum number of hours. The maximum is configured (see *User Group Details > T&A Report Tab* on page 101). • **Ignore Unpaired Events** – If this check box is selected, then if user logins/logouts are missing in the event log, ACT Enterprise ignores unpaired events for reporting purposes. For example, if the event log shows a user logging in at 08:00, logging in again at 12:30, and logging out at 16:30, ACT Enterprise ignores the unpaired 08:00 login event, resulting in a total period of 12:30–16:30. • **First Entry/Last Exit Per Day** – If this check box is selected, then ACT Enterprise considers the first user login of the day and the last user logout of the day, and ignores all interim login/logout events for reporting purposes.

Click **Generate** to generate a report according to your search criteria.

6.17.8.2 Results

The following table describes each of the columns on the **Time and Attendance** screen search results area.

Column Name	Description
No.	The unique number that identifies this user on the system. (Sortable.)

Column Name	Description
User Name	The user name. Click to view full details for this user on the **User Details** screen (see *The User Details screen* on page 89). (Sortable.)
User Group	The group this user is a member of. Click to view full details for this group on the **Group Details** screen (see *User Group Details Screen* on page 98). (Sortable.)
Log In time	The time the user logged in. (Sortable.)
Log Out time	The time the user logged out. (Sortable.)
Time	The time between log in and log out events for the user. (Sortable.)
Total Time	Report the total number of hours for the user per the **Totals** setting in the search fields. This figure appears on a separate row to avoid confusion. (Sortable.)

6.18 Settings (ACT Manage)

The **Settings** screen allows you to configure preferred settings/values for a range of functions in ACT Manage, such as the names of user fields and holidays, area limits and event filters.

This section describes the settings available in ACT Manage.

6.18.1 The Settings screen

The Settings screen has a number of tabs showing different settings for ACT Manage. For more information on these tabs, click the links below.

- **Settings > General** tab. For more information, see *Settings > General Tab* below.

- **Settings > Doors** tab. For more information, see *Settings > Doors Tab* on the facing page.

- **Settings > Lockdown** tab. For more information, see *Settings > Lockdown Tab* on page 142.

- **Settings > SMTP** tab. For more information, see *Settings > SMTP Tab* on page 142.

- **Settings > Muster Report** tab. For more information, see *Settings > Muster Report Tab* on page 143.

- **Settings > Doors Monitor Report** tab. For more information, see *Settings > Doors Monitor Report Tab* on page 144.

- **Settings > Events** tab. For more information, see *Settings > Events Tab* on page 144.

- **Settings > Schedule Log Event Purge** tab. For more information, see *Settings > Schedule Log Event Purge Tab* on page 145.

- **Settings > User Fields** tab. For more information, see *Settings > User Fields Tab* on page 145.

- **Settings > Holiday Names** tab. For more information, see *Settings > Holiday Names Tab* on page 145.

- **Settings > Area Limits** tab. For more information, see *Settings > Area Limits Tab* on page 145.

- **Settings > Card Print** tab. For more information, see *Settings > Card Print Tab* on page 145.

- **Settings > Installer** tab. For more information, see *Settings > Installer Tab* on page 147.

- **Settings > T&A Integration Tab** tab. For more information, see *Settings > T&A Integration Tab* on page 147.

- **Settings > DB Users Password Policy** tab. For more information, see *Settings > DB Users Password Policy Tab* on page 148.

6.18.2 Settings > General Tab

The following table describes the data that appears on the **Settings > General** tab in ACT Manage.

Field Name	Description
Language	The language used in the ACT Manage interface.
Export CSV Separator	The separator character used when exporting tabular data from ACT Manage. For more information, see *Exporting* on page 13.
Items Per Page	The number of items to show per page when search results are displayed. Maximum of 200.
Spot Interval	Some reports can be generated according to a spot check time. In this case, the spot interval determines the number of minutes before and after the spot check time for which data is included.

Field Name	Description
Behaviour when deleting users	Select what should happen to log data when a user is deleted from ACT Enterprise: • **Keep all events for user** • **Delete all log events for the user** **Note:** This setting does not affect data sent from ACT Enterprise to third party systems. In particular, if T&A integration is enabled, deletion rules for T&A data logged to a third party system by ACT Enterprise must be configured separately under **Settings > T&A Integration > Action on user deletion**. For more information, see *Settings > T&A Integration Tab* on page 147.
Optional Column	The default value displayed in the last column of screens showing user lists is determined by this setting (see, for example, *The Users screen* on page 87 or *User Tracking report* on page 134).
Auto Logout Time (mins)	The number of minutes after which an operator is logged out of ACT Manage if they are idle. Set to 0 to disable auto logout.
Disable Confirmation Messages	Select this check box to disable the feedback messages that appear throughout ACT Manage when an action is successful. Operators are still be prompted to confirm actions such as user deletions.

6.18.3 Settings > Doors Tab

The following table describes the data that appears on the **Settings > Doors** tab.

Field Name	Description
Fire override doors	The door group containing doors that are opened automatically via an input from the fire alarm system. In practice, this input is brought separately to each controller that is then responsible for opening any of its doors that have been defined in this group.
Anti-passback doors	The door group containing doors that are in the system's anti-passback area. Anti-passback operation is local to each controller, so if there is only one desired anti-passback area, these doors must all reside on the same controller. If the anti-passback group includes doors on more than one controller, then each controller effectively implements a separate independent area.
Auto Reset Time	If selected, then the corresponding field contains the time of the day when the anti-passback buffer is automatically reset. This ensures that users who fail to exit properly are allowed in again. If the box is unchecked, then the anti-passback buffer must be reset manually in ACT Monitor. For more information, see *Tools (ACT Monitor)* on page 158.
Perimeter doors	The door group containing doors on the perimeter of the installation. This allows the system to keep track of which users are in or out of the installation at a given time. This information is used when generating a muster report. For more information, see *User Tracking report* on page 134.
Timed anti-passback doors	The door group containing doors that do not re-open for the same card during the anti-passback timed period. For more information, see *User Group Details > Anti-passback Tab* on page 100.
Time and Attendance doors	The door group containing doors used for recording user entrances and exits for time and attendance purposes.

Field Name	Description
Internal doors	The door group containing doors inside the perimeter of the installation. These doors deny access if the cardholder has not already entered through the perimeter or anti-passback doors.
User Limit A User Limit B	These user limits may be used to generate outputs when the number of users in an area falls below a specified minimum. If user limiting is enabled, these limits specify the maximum number of users that are allowed in that area. The two limits operate independently. Refer to the controller output options for details.

6.18.4 Settings > Lockdown Tab

Select the **Enable Lockdown** check box to enable the lockdown option in ACT Enterprise. For more information on configuring and initiating/cancelling lockdowns, see *Configure and implement system lockdowns* on page 33.

The following table describes the additional fields that appear on the **Settings > Lockdown** tab. when **Enable Lockdown** is selected.

Field Name	Description
Lockdown Doors	Select the door group containing the doors that should be locked when a lockdown is initiated. For information on creating a door group, see *Add a door group* on page 27.
Allow access/exit to User Groups with Bypass option set	If selected, then cardholders in user groups with the **Tracking Bypass** option set can access/exit locked down doors. For information on configuring user group options, see *User Group Details > Options Tab* on page 99.
Allow access/exit to valid users in lockdown	If selected, then any valid user can access/exit locked down doors.
Allow Exit Button	If selected, then locked down doors open if the exit button at the door is pressed.
Allow Fire Event to unlock doors in Lockdown	If selected, then locked down doors open if there is an fire event.
Allow exit to valid cardholders	If selected, then any valid cardholder can access/exit locked down doors.

6.18.5 Settings > SMTP Tab

The settings on this tab are used when sending emails as the result of rules in ACT Manage (see *The Rule Details screen* on page 108), and when emailing the following ACT Manage reports to configured recipients:

- muster report (see *Settings > Muster Report Tab* on the facing page)
- doors monitor report (see *Settings > Doors Monitor Report Tab* on page 144)

You can also configure SMTP settings for notification emails sent by ACT Install. For more information, see *Settings > Email Notification Tab* on page 82.

The following table describes the data that appears on the **Settings > SMTP** tab.

Field Name	Description
Provider Name	Select an email provider from the **Provider Name** drop-down.
Server Name Server Port	If you select a pre-configured email provider, the **Server Name** and **Server Port** fields are populated with default details. You can edit these details if required. If you select **User Defined**, enter custom details in the **Server Name** and **Server Port** fields.
SSL Required	Select this check box if the SMTP server requires SSL.
Anonymous User	Select this check box if the SMTP server allows anonymous login. Alternatively, enter a **Username** and **Password** to authenticate to the SMTP server.
Send Test Email	Click to send a test email using this configuration.

6.18.6 Settings > Muster Report Tab

A muster report lists all users currently on site. ACT Enterprise automatically generates a muster report if a fire event is triggered onsite, and this report can be automatically printed to one or more designated printers, and emailed to several addresses, for example, the fire officers in the organisation.

The following table describes the configuration settings that appear on the **Settings > Muster Report** tab.

Field Name	Description
General	
Muster Cutoffs	Configure the conditions for clearing down muster data. Options include clearing down musters daily at a specific time, clearing down users still recorded as onsite after a threshold number of hours, and whether to clear down antipassback data and area counts.
Print by user group	Select this check box to sort the list of users on the muster report according to their user group.
Emails	
Email To Recipients	Select this check box if the muster report should be emailed to designated recipients on generation.
Recipients	Enter the email addresses for the designated recipients of the muster report. **Note:** You must configure SMTP settings under **Settings > SMTP** for this report to be emailed to the designated recipients.
Printer Settings	
You can configure Muster Reports to automatically print to one or more designated printers if there is a fire event. In this case, ACT Enterprise prints to the configured printer(s) via the LocalSystem account on the Windows machine hosting ACT Enterprise.	
For information on configuring printers for the LocalSystem account, refer to the operating system documentation.	
Print to service's default printer	Select this check box to automatically print to the default printer for the LocalSystem account. The default printer name displays on screen.

Field Name	Description
Send report to printers	Select this check box to automatically print to one or more specific printers to which the LocalSystem account has access, then select the specific printer(s) from the list of available options.
Fire Buildings	
Define buildings to split your site into different areas for the purposes of generating muster reports. Enter the building name, choose a door group with all fire doors for the building and another door group to represent the perimeter doors of the building. These settings override the general fire and perimeter door settings.	

6.18.7 Settings > Doors Monitor Report Tab

The doors monitor report is a CSV report that includes every log event on all doors in a specified door group for the reporting period. A daily report includes log events for the preceding 24 hours, and a weekly report includes log events for the preceding 7 days. It is emailed by ACT Manage to a list of specified recipients using the email settings configured under **Settings > SMTP** (see *Settings > SMTP Tab* on page 142).

The following table describes the data that appears on the **Settings > Doors Monitor Report** tab.

Field Name	Description
General	
Enable	Select this check box to enable the **Doors Monitor** report.
Custom title	Enter a custom title for the report.
Door Group	Select the door group for which the report should be generated.
Schedule	Select the schedule for the generation of this report.
	If you select **Daily**, specify the time at which the report should be generated.
	If you select **Weekly**, specify the day and time at which the report should be generated.
Emails	
Recipients	Enter the email addresses for the designated recipients of the muster report.
	Note: You must configure SMTP settings under **Settings > SMTP** for this report to be emailed to the designated recipients.

6.18.8 Settings > Events Tab

ACT Manage allows you to customise the text colour used to display different event types. This may be useful, for example, to quickly identify events of interest when viewing the **Live System** page, or the **User Tracking** or **Event Analysis** reports.

For each event type, select the colour that ACT Manage should use when displaying text relating to events of that type.

Click **Default Colours** to reset all options to the default colours.

6.18.9 Settings > Schedule Log Event Purge Tab

The following table describes the data that appears on the **Settings > Schedule Log Event Purge** tab.

Field Name	Description
Auto purge log events?	Select this check box if ACT Enterprise should automatically purge log events.

Field Name	Description
Months of log events retained	If you have selected the **Auto purge log events?** check box, specify the number of months of log events that should be retained. Log events that fall outside of this timeframe, relative to the current date, are purged.

6.18.10 Settings > User Fields Tab

This tab defines the labels that appear through the system for user fields 1–10.

See also:

- *The Users screen* on page 87
- *The User Details screen* on page 89
- *Reports (ACT Manage)* on page 130

6.18.11 Settings > Holiday Names Tab

This tab defines the labels that appear through the system for holiday types 1–9.

See also:

- *The Holidays screen* on page 112
- *Time Zone Details > General Tab* on page 111

6.18.12 Settings > Area Limits Tab

ACT Enterprise supports up to 8 different counting areas. Limits on the number of users permitted in each of these areas can be specified on this screen.

Each counting area is assigned a door group. When a valid card holder enters one of the doors in the door group the area count is incremented. When the limit is reached, then access is denied. The count is decremented when a card holder leaves through one of the doors in the door group.

Notes:

- Entry and Exit readers are required on the doors for this feature to work.
- Area limits may also be set for members of a particular user group. In this case, even if the overall area limit is not reached, if the limit for the user group is reached no more members of that user group are granted admission to the area until a group member leaves.

See also:

- *User Group Details > Area Limits Tab* on page 101

6.18.13 Settings > Card Print Tab

This page allows different encoding formats for magnetic stripe cards and barcoding profiles to be added for different cards.

The following table describes the data that appears on the **Settings > Card Print** tab.

Field Name	Description
Default Card	Select which card template to give to new user groups. This list is populated with options read from the **Card Templates** folder selected below.

Field Name	Description
Card Templates	Click **...** to open a dialog where you can browse to and select the folder with card templates. Card templates are XML format files added by default to the following folder on the ACT Enterprise server: C:\ProgramData\Access Control Technology\ACT Enterprise\Publish\Clients\CardEditor\CardTemplates
Encoding Profiles	Which encoding profiles are available. For each profile, the profile name and encoded tracks are indicated. Click **Add** to add a new profile, or select a profile and click **Edit** to edit an existing profile. For more information, see *The Encoding Profile screen* below.
Barcode Profiles	Which barcode profiles are available. Click **Add** to add a new profile, or select a profile and click **Edit** to edit an existing profile. For more information, see *The Barcode Profile screen* below.

6.18.14 The Encoding Profile screen

Please refer to the card manufacturer's technical specifications or MIFARE card reader specifications for more information on encoding settings.

6.18.15 The Barcode Profile screen

The following table describes the data that appears on the **Barcode Profile** screen.

A preview of a sample barcode in the top right area of the screen reflects the profile settings.

Note: Standard ACT magnetic stripe cards are encoded on Track 2 only.

Field Name	Description
Profile Name	The name of the barcode profile.
Symbology	The barcode style generated when this profile is used.
Barcode Data	Specify the static and variable values to be included in the barcode.
Show Readable Text	If selected, readable text is displayed on the barcode.
Bearer Bars	If selected, bars appear at the top and bottom of the barcode if the barcode symbology supports them.
Quiet Zones	If selected, additional whitespace is added to the barcode to provide a distinct boundary.
Text On Top	If selected, any displayed text appears above the barcode instead of below.
Rotation	The degree to which the barcode should be rotated.
Narrow Bar Width	The width of narrow bars in barcodes that show a series of side-by-side bars.
Bar Height	The height of bars in barcodes that show a series of side-by-side bars.

6.18.16 Settings > Installer Tab

This tab shows the name and a brief description for the current ACT Enterprise installation.

6.18.17 Settings > T&A Integration Tab

The following table describes the data that appears on the **Settings > T&A Integration** tab.

Field Name	Description
Options	
Activation Date and Time	Specify the date and time from which T&A data should be logged by ACT Enterprise. No punch events are transmitted before this time.
T&A Doors	Select the door group that includes the entry and exit readers used to determine when users in this group are considered logged in/out for T&A purposes.
	This can be overridden for an individual user under **Manage > Users > User Details > T&A Integration**. For more information, see *User Details > T&A Integration Tab* on page 93.
User field defining Email	Select which user fields on the **User Details > Details** screen contains the email address, title, phone number and address of the user.
User field defining Title	The fields on the **User Details > Details** screen are customisable at a per-system level. For more information, see *User Details > Details Tab* on page 91 and *Settings > User Fields Tab* on page 145.
User field defining Phone	
User field defining Address 1	
Action on user deletion	Select what action should be taken in the third party T&A software when a user is deleted in ACT Enterprise: the user in the T&A software can be deleted, disabled or left as is.
	Note: This setting is independent of the **Settings > General > Behaviour when deleting users** setting, which applies to ACT Enterprise log information only. For more information, see *Settings > General Tab* on page 140.
Communication	
VisionTime	Select the check box to enable integration with VisionTime, a third party T&A software.
	If VisionTime integration is enabled, enter the web address and login credentials for the service.
Advanced	
The options on this tab allow you to resend, synchronise and export T&A punch events if there is a communications failure between ACT Enterprise and the VisionTime server. Because data may be overwritten, and log in/log out mismatches may be introduced if this function is used incorrectly, Vanderbilt recommends that you only use these functions if you have received training on ACT Enterprise T&A integration, and that you backup your ACT Enterprise and VisionTime databases before using these functions.	

ACT Enterprise can also generate a basic report, based on events at entry and exit doors in the system. For more information on T&A options in ACT Enterprise, see *Report on time and attendance (T&A)* on page 45.

6.18.18 Settings > DB Users Password Policy Tab

The following table describes the data that appears on the **Settings > DB Users Password** tab.

Field Name	Description
Enable Password Policy	Select this check box to enable a password policy for ACT Enterprise in your organisation.
Password Complexity	Set parameters to define the minimum password complexity required.
Password Management	Set the maximum number of times a DB user can enter an incorrect password before their account is locked, and select the lockout duration.
	To protect against lockout if you lose or forget the admin password for your installation of ACT Enterprise, you can optionally select the **Allow admin password of the day access** check box. In this case, if you are locked out, you can contact Vanderbilt technical support to request a time-limited, generated password that unlocks the system.

6.18.19 Settings > Mobile Access Tab

The following table describes the data that appears on the **Settings > Mobile Access** tab.

Field Name	Description
Enable	Select this check box to enable mobile app support in ACT Enterprise.
	Note: This check box is disabled if a strong password policy is not enabled under **Settings > DB Users Password Policy**.
Azure connection	ACT Enterprise must be able to connect to the internet (and specifically to Microsoft Azure) to support connections from the mobile app.
Unique Identifier	Displays a system-generated **Unique Identifier**. Authorised DB users must enter this identifier in the ACT Enterprise mobile app to access your system.
Site Description	Enter a **Site Description**. This will display on the mobile app interface.

6.19 Clients (ACT Manage)

Click any of the client software options in the **Clients** menu to open the corresponding software module for ACT Enterprise. The selected module opens in front of the current module.

You must have logon access to use each client, and which tasks you can perform depends on the access rights you have been granted.

The following options are available (if you have full access rights) on the ACT Manage **Clients** menu.

- **ACT Install**. For more information, see *About ACT Install* on page 53.

- **ACT Monitor**. For more information, see *About ACT Monitor* on page 150.

- **ACT Server Client**. For more information, see *About ACT ServerClient* on page 48.

- **ACT SiteMaps Editor**. ACT SiteMaps Editor is a visual designer tool that creates a list of maps from pre-designed graphics that represent infrastructure units of an access control site, and places ACT controlling units (doors, inputs/outputs, etc.) on those maps according to their physical location in the building. For more information, please refer to the online help included in ACT SiteMaps Editor.

- **ACT SiteMaps Monitor**. ACT SiteMaps Monitor is an optional add-on to the ACT Enterprise system. It is a real-time access control tool that provides visual navigation through the system of

maps created with ACT SiteMaps Editor, allows you to issue basic commands on access control objects on the maps, and allows you to monitor events and status changes from the ACT system via maps in live mode. For more information, please refer to the online help included in ACT SiteMaps Monitor.

7 ACT Monitor Reference

This section describes the following:

See also:

7.1 About ACT Monitor

ACT Monitor allows security and reception staff to monitor activity on the system and to easily issue door commands.

> ⓘ   ACT Enterprise Lite (free) does not support the ACT Monitor client.

Events can be viewed for doors and for users. More complex reporting is also possible. Live events appear in the home page and the information stream can be paused to allow closer inspection of one or more specific events. A list of doors can be filtered by user group or status. Alarms are listed in a separate panel, where they can be acknowledged if desired.
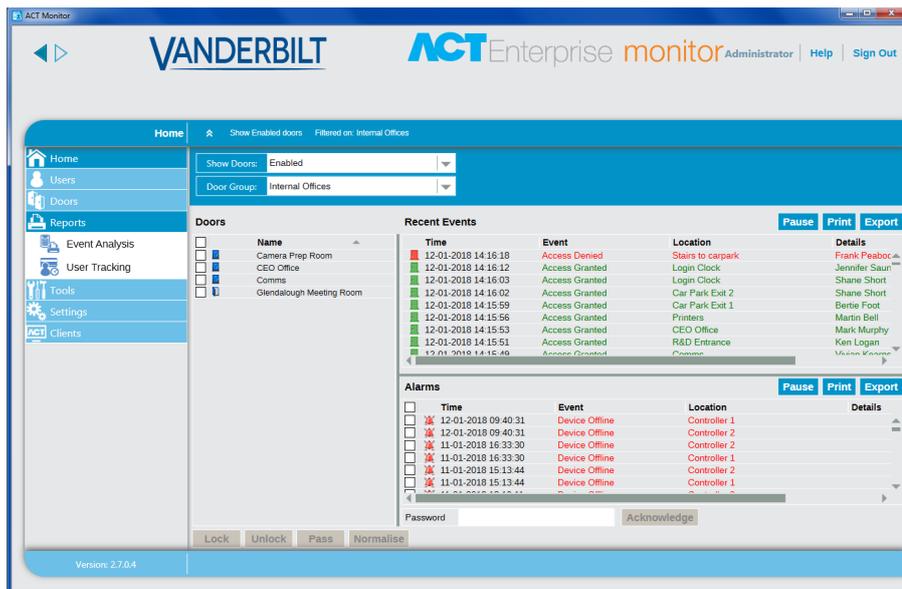
7.2 The ACT Monitor Home screen

The **Home** screen provides a summary view of the ACT Enterprise system.

- **Doors.** This area shows the status of all doors on the system. Hover over the icon for any door to see its status in a popup. You can issue a command on a door by selecting the box for that door, then clicking **Lock**, **Unlock**, **Pass** or **Normalise** at the bottom of the screen.

  You can use the **View Options** to filter the doors you can see in the panel by several criteria. You can view doors that are Online or Offline, Enabled or Disabled. Or you can choose a specific door group to view (this option filters the recent events displayed also).

- **Recent Events.** This area shows the time, location and summary information for events on the system.

  Click **Pause** to temporarily prevent new events from appearing in this area – this may be of use if there are a high volume of events and you want to read the details for one currently on screen. The **Pause** button turns into a **Continue** button when pressed. Click **Continue** to begin adding live events to this area again.

  You can filter the events you can see by selecting a specific **Door Group** in the **View Options** area.

  You can also print and export information displayed in this area. For more information, see *Printing* on page 13 and *Exporting* on page 13.

  For an event involving a user, such as an **Access Granted** or **Access Denied** event, click the user's name in the **Details** column to view the user's profile on the **User Details** screen. Click the **Back** icon () at the top of the **User Details** screen to return to the **Home** screen.

- **Alarms.** This area shows alarms that have been triggered on the system.

  As with the **Recent Events** area, you can pause, print and export the data shown here.

  Click a value in the **Event** column to view that event on the **Event Details** screen (see *The Event Details screen* below).

  You can also mark an alarm as **Acknowledged**, which indicates that you have seen the alarm details and either taken action, or determined that no action is required. Acknowledged alarms are removed from this area. To acknowledge an alarm, select the box for that alarm, enter a password if necessary, and click **Acknowledge**.

If lockdowns have been enabled and configured, you can initiate and clear lockdowns from this screen as follows:

- To initiate a lockdown, click **Lockdown**. All doors in the door group specified under **Lockdown Doors** on the **Settings > Lockdown** tab in ACT Manage are locked down.

- To cancel a lockdown, click **Clear Lockdown**. All doors return to their previous state.

7.3 The Event Details screen

This screen shows the time and location of a specified event.

You can mark an alarm as **Acknowledged**, which indicates that you have seen the alarm details and either taken action, or determined that no action is required.

To acknowledge an alarm event, enter a password if necessary, and click **Acknowledge**.

7.4 Users (ACT Monitor)

Users are access control card holders. The system allows you to view user details, monitor the activities of users, and manually log users in and out.

The following sections describe the functions available in this menu:

See also:

- *The ACT Monitor Home screen* on page 150
- *Reports (ACT Monitor)* on page 155

7.4.1 The Users screen

The **Users** screen is accessed through the **Users** menu item in ACT Monitor.

See also:

- *Search Fields* below
- *Results* on the next page

7.4.1.1 Search Fields

Field Name	Description
Search	Enter all or part of the registered name for the user whose record you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area. **Example:** Searching for "Ann" might show results for "**Ann**-Marie Boyle", "Jo**ann**e Murphy", and "Joseph H**ann**".
Advanced. Click **Advanced** to see the following additional search fields. You can use one or more fields to specify your search criteria.	
User Number	Enter the user number. The system returns an exact match if found.
First Name	Enter all or part of the user's first name.
Last Name	Enter all or part of the user's last name.
Group	Select the group to which the user is assigned.
Card number	Enter the user card number. The system returns an exact match if found.
State	Select the user state: **Enabled**, **Disabled** or **All** (either).
Selectable field	At the final search field, select one additional user field to search on, and enter matching text.

7.4.1.2 Results

The following table describes each of the columns on the **Users** screen search results area.

Column Name	Description
No.	The unique number that identifies this user on the system. (Sortable.)
Name	The user's name. (Sortable.)
	Click a user's name to view the user's profile on the **User Details** screen (see *The User Details screen* below). Click the **Back** icon (◀) at the top of the **User Details** screen to return to the **Users** screen.
Enabled	A green check mark is shown here if the user is enabled on the system.
Group	The group this user is a member of. (Sortable.)
Location	The user's current location, if available.

7.4.2 The User Details screen

The following table describes the data that appears on the **User Details** screen in ACT Monitor.

Click the **Previous** (◀) and **Next** (▶) buttons at the bottom of the screen to page through user records.

Field Name	Description
Photo	If a photo of the user has been added to the system, it appears here.
User Number	The user's number.
User Name	The user's name.
User Group	The group this user is a member of.
Status	Whether this user is **Enabled** or **Disabled** on the system.
Valid From	The start of this user's validity period, if set.
Valid To	The end of this user's validity period, if set.
Manual Login	Click to open the **Manual Login** screen where you can manually log the user in to the system (see *The Manual Login screen* on the facing page).
Manual Logout	Click to open the **Manual Logout** screen where you can manually log the user out of the system (see *The Manual Logout screen* on the facing page).
General tab	
Last Event	For the last event for this user, the event name, time and location is displayed.
Recent Events	This area shows a list of recent events recorded for the user, including the event name, time, location and details for each one.
Monitor User	If selected, this user is monitored. The **Advanced** settings on the **User Tracking** screen allow you to generate reports on monitored users (see *User Tracking Screen* on page 156).
Verify Visually	If selected, this user should be verified visually at challenge doors.

Field Name	Description
Details tab	
User Fields	The 10 user fields are customisable per ACT Enterprise installation. The field labels indicate the types of information recorded for this user on your system.
Cards	Numbers of the card(s) registered for this user.
View Doors tab	
This tab shows a list of door/time zone combinations valid for this user. A user can only access a door during the period specified by the associated time zone.	
The **Source** column indicates the primary source of each door/time zone combination. This may be the user's User Group, Extra Rights, or Door Plan.	

7.4.3 The Manual Login screen

You may occasionally need to manually log a user in to the system, for example, if they have forgotten their card. User login data enables ACT Enterprise to generate accurate muster reports, and time and attendance reports. The **Manual Login** screen allows you to log a user in to the system.

To access this screen, click **Manual Login** on the **User Details** screen in ACT Monitor or ACT Manage. You are prompted to specify whether you want the login to be recorded **Now**, or from a **Custom** date/time on the **Manual Login** screen. Specify the required login time and click **Log In**.

7.4.4 The Manual Logout screen

You may occasionally need to manually log a user out of the system, for example, if they have forgotten their card. User logout data enables ACT Enterprise to generate accurate muster reports, and time and attendance reports. The **Manual Logout** screen allows you to log a user out of the system.

To access this screen, click **Manual Logout** on the **User Details** screen in ACT Monitor or ACT Manage. You are prompted to specify whether you want the logout to be recorded **Now**, or from a **Custom** date/time on the **Manual Logout** screen. Specify the required logout time and click **Log Out**.

7.5 Doors (ACT Monitor)

The **Doors** screen is accessed through the **Doors** menu item in ACT Monitor.

See also:

- *Search Fields* below
- *Results* on the next page

Note: You can issue a command on a door from this screen by selecting the box for that door in the search results area, then clicking **Lock**, **Unlock**, **Pass** or **Normalise** at the bottom of the screen.

7.5.1 Search Fields

Field Name	Description
Search	Enter all or part of the name of the door whose details you want to view and click the **Search** icon (🔍). A list of matching records is displayed in the **Search Results** area.
Advanced. Click **Advanced** to see the following additional search fields.	
Door Number	Enter the door number. The system returns an exact match if found.
Door Name	Enter all or part of the door name.

Field Name	Description
Group	Select the group to which the door is assigned.

7.5.2 Results

The following table describes each of the columns on the **Doors** screen search results area.

Column Name	Description
No.	The unique number that identifies this door on the system. (Sortable.)
Name	The door's name. Click to view a report on activity at this door on the **Event Analysis** screen (see *Event Analysis Screen* below). (Sortable.)
State	The door's current state, for example online or offline. Hover your mouse over the door icon in this column to see the state in a popup.
Last event	Summary information on the last event recorded at the corresponding door, for example **Access Granted** or **Exit Button Used**. (Sortable.)

7.6 Reports (ACT Monitor)

ACT Monitor allows you to generate a number of reports on ACT Enterprise events according to specific criteria. This section describes the report types available.

7.6.1 Event Analysis Screen

The **Event Analysis** screen is accessed through the **Reports > Event Analysis** menu item in ACT Monitor.

See also:

- *Search Fields* below
- *Results* on the facing page

7.6.1.1 Search Fields

The following table describes the **Simple** and **Advanced** search fields available on the **Event Analysis** screen.

Note: Click **Refresh** at the top of this screen at any time to update the report with the latest data.

Field Name	Description
Simple Tab Filter	
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: - **All** – all users. - **Single** – select a particular user on the **User Lookup** screen (see *The User Lookup screen* on page 14).

Field Name	Description
Time	Select whether to generate the report for **Today,** a particular time (**Spot Check**) or a **Custom** time period. A **Spot Check** report includes a time period either side of the specified time – this is specified by the **Spot interval** value on the **Settings > Events** tab (see *Settings > Events Tab* on page 159).
Advanced Tab Filter	
Events	Select particular event types to report on.
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: ● **All** – all users. ● **Single** – select a particular user on the **User Lookup** screen (see *The User Lookup screen* on page 14). ● **Belonging to User Group** – select a particular user group.
Doors	Select criteria for doors to report on by choosing from one of the following options and entering additional information in any fields that appear: ● **All** – all doors. ● **Single** – select a particular door. ● **Belonging to Door Group** – select a particular door group.
Time	Select whether to generate the report for **Today, This Week, This Month, Spot Check** or a **Custom** time period. A **Spot Check** report includes a time period either side of the specified time – this is specified by the **Spot interval** value on the **Settings > Events** tab (see *Settings > Events Tab* on page 159).

Click **Generate** to generate a report according to your search criteria.

7.6.1.2 Results

The following table describes each of the columns on the **Event Analysis** screen search results area.

Column Name	Description
Time	The event time. (Sortable.)
Event	The event type. (Sortable.)
Location	The location (controller/door) of the event. (Sortable.)
Details	Details about the event. For events associated with a user, click the user name to view details about that user on the **User Details** screen (see *The User Details screen* on page 153). (Sortable.)

7.6.2 User Tracking Screen

The **User Tracking** report is accessed through the **Reports > User Tracking** menu item in ACT Monitor.

See also:

● *Search Fields* on the next page

● *Results* on the next page

Note: Click **Refresh** at the top of this screen at any time to update the report with the latest data.

7.6.2.1 Search Fields

Field Name	Description
Simple	
Report	Select whether to generate a **Muster** report (all users currently on site), or an **Absentee List** report (users not on site).
Time	Select whether to generate the report for **Today,** or a **Custom** time period.
Advanced	
Report	Select which report type to generate. • **Muster** – all users currently on site • **Last Entry** – the last point of entry for users • **Last Entry or Exit** – the last point of entry or exit for users • **Last Location** – the last known location of users • **Absentee List** – users not on site. Reports on absent users provide information on the last known event and time for absentees where such details are available.
Doors	Select criteria for doors to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all doors. • **Single** – select a particular door. • **Belonging to Door Group** – select a particular door group.
Users	Select criteria for users to report on by choosing from one of the following options and entering additional information in any fields that appear: • **All** – all users. • **Single** – select a particular user on the **User Lookup** screen (see *The User Lookup screen* on page 14). • **Belonging to User Group** – select a particular user group.
Options	To include user photos (if available) in the report results, select **Show photo**. To include enabled users only in the report results, select **Show enabled users only**.
Time	Select whether to generate the report for **Today, This Week, This Month,** or a **Custom** time period.

Click **Generate** to generate a report according to your search criteria.

7.6.2.2 Results

The following table describes each of the columns on the **User Tracking** screen search results area.

Column Name	Description
Time	The event time. (Sortable.)
Event	The event type. Click to view information about this event on the **Event Details** screen. (Sortable.)
Location	The location (controller/door) of the event. (Sortable.)

Column Name	Description
Details	The user connected to the event. Click the user name to view details about that user on the **User Details** screen (see *The User Details screen* on page 153). (Sortable.)

7.7 Tools (ACT Monitor)

The **Tools** menu in ACT Monitor enables you to access the following tools:

- **Reset Muster** – Click to reset the muster list. This effectively logs all users out of the system for muster reporting purposes.

- **Reset Anti-passback** – Click to reset anti-passback memory on controllers system-wide. This effectively logs all users out of anti-passback areas.

- **Reset Area Counts** – Click to reset area counts system-wide. For more information on area counts and limits, see *Settings > Area Limits Tab* on page 145.

7.8 Settings (ACT Monitor)

The **Settings** screen allows you to configure preferred settings/values for a range of functions in ACT Monitor, such as which doors are challenge doors, and what colours are used for different event types in reports.

This section describes the settings available in ACT Monitor.

7.8.1 The Settings screen

The **Settings** screen has a number of tabs showing different settings for ACT Monitor. For more information on these tabs, click the links below.

- **General** tab. For more information, see *Settings > General Tab* below.

- **Events** tab. For more information, see *Settings > Events Tab* on the next page.

- **Challenge** tab. For more information, see *Settings > Challenge Tab* on the next page.

- **Installer** tab. For more information, see *Settings > Installer Tab* on page 160.

7.8.2 Settings > General Tab

The following table describes the data that appears on the **Settings > General** tab.

Field Name	Description
Language	The language used in the ACT Monitor interface.
Export CSV Separator	The separator character used when exporting tabular data from ACT Monitor. For more information, see *Exporting* on page 13.
Items Per Page	The number of items to show per page when search results are displayed.

Field Name	Description
Spot Interval	Some reports can be generated according to a spot check time. In this case, the spot interval determines the number of minutes before and after the spot check time for which data is included.
Optional Column	The default value displayed in the last column of screens showing user lists is determined by this setting.
Auto Logout Time (mins)	The number of minutes after which an operator is logged out of ACT Monitor if they are idle. Set to 0 to disable auto logout (default).

7.8.3 Settings > Events Tab

The following table describes the data that appears on the **Settings > Events** tab.

Field Name	Description
Event Colours	What colours are used for different event types in reports.
Play Sound on Alarm	If selected, ACT Monitor plays a sound when an alarm is triggered. Select the sound from the list below.
Play Sound Continuously Until Acknowledgement	If selected, ACT Monitor continues to play an alarm sound until the alarm has been acknowledged. For more information on acknowledging alarms, see *The ACT Monitor Home screen* on page 150. Select the sound from the list below.

7.8.4 Settings > Challenge Tab

The following table describes the data that appears on the **Settings > Challenge** tab.

Field Name	Description
Challenge Doors	The door group that contains challenge doors.
Auto-acknowledge	When a user with the **Verify Visually** option passes through a challenge door, the user's image appears onscreen. The image remains onscreen for the number of minutes specified here.
Events	The selected event types generate alerts at challenge doors.
Operate challenge on timezone	The challenge feature is enabled during the selected timezone.
Display user field	Data from the selected user field is displayed when a user passes through a challenge door.
Play sound on challenge	If selected, ACT Monitor plays a sound when a user passes through a challenge door. Select the sound below.
Play sound continuously until acknowledgement	If selected, ACT Monitor continues to play a sound when a user passes through a challenge door, until the event has been acknowledged. For more information on acknowledging events, see *The ACT Monitor Home screen* on page 150. Select the sound from the list below.

7.8.5 The Challenge screen

Challenge doors are configured under the **Settings > Challenge** tab (see *Settings > Challenge Tab* above).

When a user event that has been configured to generate an alert at a challenge door occurs, details of the event type, time, location and phone number, and details of the user that triggered the challenge appear on the **Challenge** screen.

Depending on the options selected on the **Settings > Challenge** tab, a sound may be played when an alert is triggered, and a video of activity at the door may be displayed.

You should select whether to **Allow** or **Deny** the event by selecting the appropriate check box, then click **Acknowledge**.

7.8.6 Settings > Installer Tab

This tab shows the name and a brief description for the current ACT Enterprise installation.

7.9 Clients (ACT Monitor)

Click any of the client software options in the **Clients** menu to open the corresponding software module for ACT Enterprise. The selected module opens in front of the current module.

You must have logon access to use each client, and which tasks you can perform depends on the access rights you have been granted.

The following options are available (if you have full access rights) on the ACT Monitor **Clients** menu.

- **ACT Install**. For more information, see *About ACT Install* on page 53.

- **ACT Manage**. For more information, see *About ACT Manage* on page 85.

- **ACT SiteMaps Editor**. ACT SiteMaps Editor is a visual designer tool that creates a list of maps from pre-designed graphics that represent infrastructure units of an access control site, and places ACT controlling units (doors, inputs/outputs, etc.) on those maps according to their physical location in the building. For more information, please refer to the online help included in ACT SiteMaps Editor.

- **ACT SiteMaps Monitor**. ACT SiteMaps Monitor is an optional add-on to the ACT Enterprise system. It is a real-time access control tool that provides visual navigation through the system of maps created with ACT SiteMaps Editor, allows you to issue basic commands on access control objects on the maps, and allows you to monitor events and status changes from the ACT system via maps in live mode. For more information, please refer to the online help included in ACT SiteMaps Monitor.

VANDERBILT