

Understanding Access Rights in CELCAT[®] Timetabler 6

Introduction

CELCAT *Timetabler* 6 software employs in-built permissions-based security to control access to timetable data such as rooms, staff, events, etc. This access control is configured and maintained by the CELCAT *Timetabler* Administrator application, and enforced by all CELCAT applications that require use of the timetable data.

The screenshot shows the 'Users' page in the CELCAT Timetabler Administrator application. The interface includes a navigation menu at the top with tabs for 'General', 'Settings', 'Users', 'Roles', 'Week Schemes', 'Terminology', 'Enforced Preferences', and 'User Authentication'. The 'Users' tab is selected, and the 'Details' sub-tab is active. The main area contains a form for user details. The 'User name' field is filled with 'ala101'. The 'Staff name' and 'Department' fields are empty. The 'Student name' field is filled with 'Truong, Alan'. The 'NT user name' field is empty. There is a 'Set Password...' button next to the 'User name' field. Under the 'Password security' section, the 'Can change password' radio button is selected. There are also checkboxes for 'Active' and 'Rooming administrator'. A status box at the bottom right indicates the user was last updated on 19/06/2006 at 15:18:51. The bottom status bar shows 'Browse mode' and 'Not logged in'.

Figure 1 - *Timetabler Administrator Users Page*

This document describes how access rights affect the authority of *Timetabler* users. Please see the *Getting Started Guide* for instructions on creating users, roles and access rights in the *Timetabler Administrator* application. The *Getting Started Guide* can be found at:

<http://www.celcat.com/products/timetabling/pdfs/CT6GettingStartedGuide.pdf>

The features described in this document apply to the latest revision of *Timetabler 6* software and may differ from those implemented in earlier releases.

Terminology

A brief definition is given for each of the following frequently-used terms:

Timetabler	CELCAT <i>Timetabler</i> 6 software
User	A user of the <i>Timetabler</i> software
Role	A role that is assumed by a user during login and that dictates his access rights
Administrator Role	A role with administrative capacity, unrestricted by access rights
Attribute	The nature of a particular permission or restriction that is applied by the security model, e.g. <i>Deny</i> , <i>View</i> , <i>Modify</i> etc
Permission Level	The level at which access rights are applied, e.g. timetable-wide, by department, etc

Aspect	The type of data that is being secured by given access rights, e.g. resource records, staff timetables, room statistics, etc
Ownership	Most data is categorised by department leading to the notion of a record being 'owned' by a particular department

A *User's* access rights are determined by their *Role*. Each access right is defined by an *Attribute*, which is applied to an *Aspect* of the timetable data at a designated *Permission Level*.

Quick Examples

The following brief examples illustrate the extent to which security attributes can be applied to your timetable data:

1. Room Booker in Sociology Department

Alan Howard is responsible for ad-hoc room booking in the Sociology department. His access rights prevent him from viewing resources and timetables that belong to other departments. He can view staff records in his own department, but can't modify them. He can create events for the Sociology rooms.

2. Timetable Planner in Engineering Faculty

Sue Grant constructs the teaching timetable for the Engineering Faculty consisting of the Electrical Engineering and Mechanical Engineering departments. She has full access to all resources in both departments and full access to the timetables of several named staff in the Maths department who cross-teach in Engineering.

3. Human Resources Officer

Angela White is the College H.R. officer and she has full access to all staff records, and view access to their timetables. However, she has no access to any other resources (such as rooms, modules, etc).

Users and Roles

Users logon to the *Timetabler* system with a username and password, which together identify their *user* account. Additionally, each user account has one or more associated *roles*. Access rights are configured for roles rather than individual users, and this subtlety makes application of access rights very flexible.

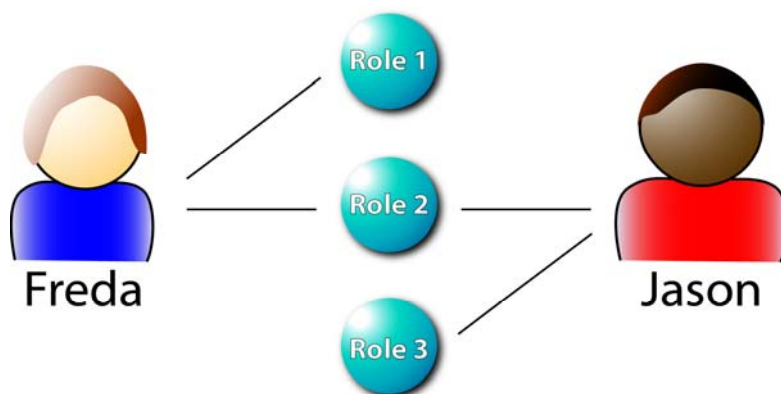


Figure 2 – Users and Roles

Note that when a user logs on to the *Timetabler* system, he does so using one of his roles, which then dictates his access rights. Although access rights are specified for roles, we often speak of a *user* as having been granted certain rights. This is simply for clarity and you should understand that these rights are assigned to the user via his chosen role.

Figure 3 - Timetabler Administrator Roles Page

Permission Levels

Access rights can be applied at the following four levels:

1. **By Timetable**

Access rights applied at this level operate on the whole of a timetable database.

2. **By Type**

Here an access rights is applied in general to all data of a particular type. For example, 'view' access may be granted to all rooms or to all staff.

3. **By Department**

Access rights applied *By Department* pertain to data of a given type in a particular department. For example, a user may be granted full access to all room data in the Department of Physics or all staff data in the Maths Department. This permission level only applies to entities which have a department attribute (all 7 resources, events and courses).

4. **By Item**

This level is used to apply access rights to an individual item in the timetable, such as an item of equipment, a room or a member of staff. The level does not apply to individual events.

A user's permissions will likely comprise access rights applied from several levels and this can give rise to apparent conflicts. For example if a user has full access to all rooms (using the *By Type* level) and view-only access to all rooms in the Music Department (using the *By Department* level) what access rights does she have to Music's rooms? Although the access rights appear contradictory, there is a simple solution – permission levels operate in a hierarchical manner as shown below, with access rights specified at a lower level overriding those at a higher level:

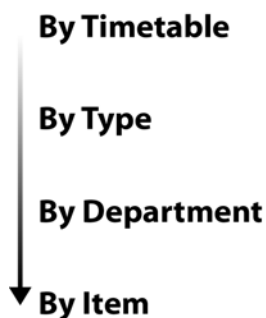


Figure 4 – Permission Levels Hierarchy

Thus, access rights applied at a *By Item* level override those at a *By Department* level, which in turn override *By Type* permissions, which again override *By Timetable* access rights. So in the scenario mentioned above, a user with full access to all rooms (i.e. a *By Type* access right), but view-only access to rooms in the music department (i.e. the lower level *By Department* access right) will find they have full access to all rooms except those in the music department, for which they will have view-only access.

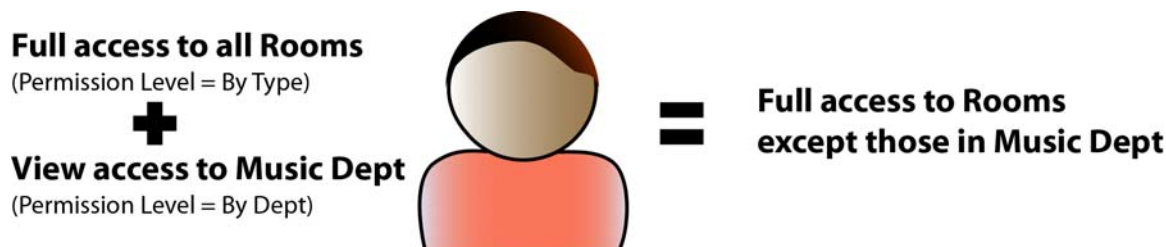


Figure 5 – Combined Permission Levels

Attribute

The access attribute describes the nature of a particular permission or restriction that is applied by the access rights mechanism. The six attributes are listed below along with their abbreviations:

Abbreviation	Attribute
X	Deny
V	View
M	Modify + View
C	Create + Modify + View
D	Delete + Create + Modify + View
A	All (usually the same as 'D' but sometimes 'M' depending on aspect)

Figure 6 – Access Attributes

The attributes are largely self-explanatory, but it is worth noting that the *Deny* attribute is unique in that it represents a restriction rather than a permission. It is a severe attribute that prevents users from even viewing data that is classified in this way (with the exception of a record's *Name* and *Unique Name* fields which are always visible).

Aspects

Access rights may be configured separately for *Records*, *Timetables*, *Statistics*, *Registers* and *Attendance* thus providing a fine degree of control over the security of your timetable data, and making it possible, for example, to *Deny* a user access to staff records but allow them to *View* staff timetables. These areas of access control are called *aspects*.

Record Aspect

Record-based rights control access to core data about resources, classifications and events. For example, a user with *All* access (i.e. attribute 'A') to a student record can change their name, telephone number, date of birth, department, tutor and so on – the basic student record data. All of the access attributes (X, V, M, C, D and A) are applicable to record data, with the following 2 exceptions:

1. Event details cannot be assigned *Deny* (X) access – you cannot prevent users from viewing events, but you can restrict the context in which they see them (see below under *Timetable* Rights). Note that *Event Detail* Rights apply solely to the 'detail' of an event and do *not* affect the ability of a user to modify an event's resources (e.g. to change the room of an event); see below under *Events* for more information.
2. Classifications cannot be assigned *Deny* (X) access.

Timetable Aspect

Timetable-based rights control access to resource timetables. For example, a user with *Deny* access to Joe Gibson's timetable is unable to display or print it. However, individual events from Joe's timetable may be visible to the user in another context, perhaps from a room timetable. The user may even be able to modify the event by changing the allocated room, but without *Modify* (M) access to Joe's timetable the user is unable to change the day it runs on, remove Joe from the event, delete the event, etc because all of these actions significantly modify Joe's timetable. The *Deny* (X), *View* (V) and *Modify* (M) attributes are applicable to timetable rights.

Statistics Aspect

Statistics-based rights control access to *Timetabler's* statistical reports and to resource-based attendance reports. A user with *View* statistics access to Room A101, for example is able to display and print statistics for it. The only applicable access attributes for statistics are *Deny* (X) and *View* (V). *Deny* may be a useful attribute to apply to sensitive statistical data, but it does not prevent users from viewing and modifying record data, etc.

Note that the *Modify* (M) attribute is not applicable to statistics.

Register Aspect

The *Register* and *Attendance* aspects are used by CELCAT's electronic student register software (called *Timetabler* SAT). A prerequisite for any use of SAT functions is that the user has the special "May use SAT" attribute set in *Timetabler* Administrator.

Register-based rights are only applicable to staff resources, and control whether or not a user can view registers. Access rights for an individual register depend purely on the list of staff assigned to the register (not on the register's department nor on the Attendance aspect described below).

Notes:

Where no members of staff are assigned to a register, users have *View* (V) access to the register. If the user also has the special "May mark own

registers” attribute then he is also able to mark such ‘unowned’ registers (*Modify (M)* attribute).

If the user is also a member of staff (this can be configured in the Administrator *Users* page), then he will always have at least *View* access to his registers (i.e. those he’s assigned to). Furthermore, if the user has the special “May mark own registers” attribute then he is also able to mark such registers (*Modify (M)* attribute).

This mechanism ensures that staff can always view or mark their own registers, even if they have restrictions on other registers. This means that a number of users may share a single role and still be able to mark their own registers but not each other’s.

Even with the *Modify* attribute, users may still be prevented from marking students on a register as ‘Withdrawn’, or from removing them altogether from a register. These rights depend upon the special “May withdraw students” and “May remove students” attributes which can be specified in *Timetabler* Administrator.

Where more than one member of staff is assigned to a register, access rights are combined so as to provide the most relaxed restrictions.

Attendance Aspect

Attendance-based rights are only applicable to events, and control whether a user can *View (V)* attendance reports or if they are *Denied (X)* from doing so. However, the *Deny* attribute does not prevent a user from viewing or modifying a register – it simply prevents access to SAT reports.

Request Aspect

Requests-based rights are only applicable to rooms, and control whether a rooming administrator user is considered to be a rooming administrator for a particular room or set of rooms, for rooms within a department, or for all rooms.

See below under “Access Rights and Printing” for more information.

Events

Permissions to modify events deserve a special mention because they are determined by a combination of both *Event Detail* rights and *Timetable* rights. A user requires sufficient permissions in both areas in order to change an event. *Timetabler* security considers that there are essentially two types of event modifications; changes to the ‘detail’ of an event and changes to an event’s resources, as depicted below:

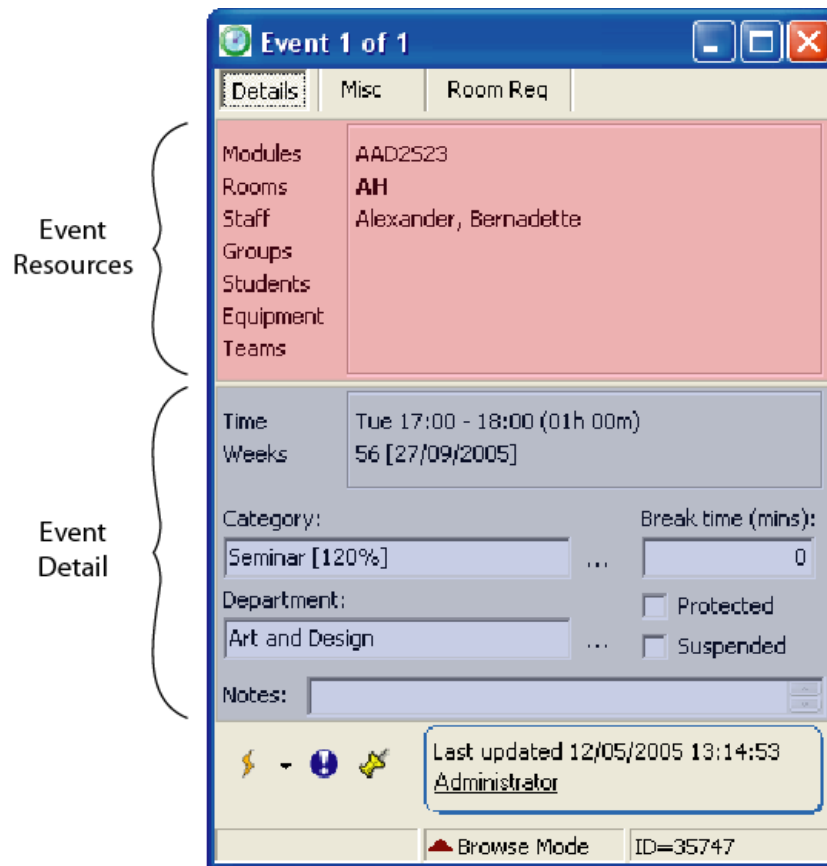


Figure 7 – Elements of an Event

The above diagram uses the *Timetabler* Client event window to depict the two basic elements of an event. Don't worry if you are not familiar with the Client software; the main thing to remember here is that a *Timetabler* event can be thought of as comprising a main 'event detail' section and another part containing the resources attached to the event.

Furthermore, within the detail of an event it is also possible to identify temporal changes – modifications to those elements of an event affecting the time at which the event takes place (the day, times, weeks, break time and suspended status as shown below). It is important to carefully control changes to an event's temporal elements because these effectively modify the timetable for all resources allocated to the event.

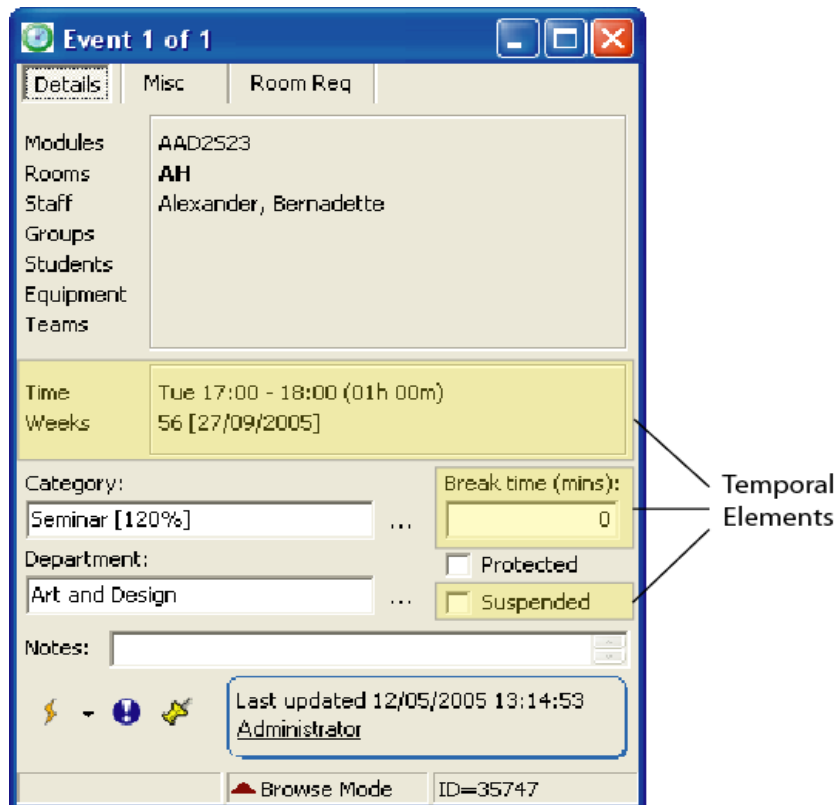


Figure 8 – Temporal Elements

Here are two rules of thumb that apply to event modification:

1. To modify the detail of an event (shown in blue in Fig 7), you need *Modify Event Details* rights. If the changes involve temporal elements of the event (shown in yellow in Fig 8), you also require *Modify Timetable* rights for all of the event's resources.
2. To modify the event resources (shown in red in Fig 7), you need *Modify Timetable* rights (but not *Modify Event Detail* rights)

Some examples serve to illustrate how *Event Detail* and *Timetable* rights unite to enforce event security:

- To create an event for room G101, a user needs *Create Event Detail* rights (to create the detail of the event), and also *Modify Timetable* rights for G101 (the event's only resource). To delete this newly-created event, the user requires *Delete Event Detail* rights (to delete the detail of the event), and also *Modify Timetable* rights for the event resource – room G101.
- To change an event from room G101 to G102 the user needs *Modify Timetable* rights for both G101 and G102. Note, however, that *Modify Event Detail* rights is *not* required, because the user is only changing the event's resources not the detail of the event.
- To change ownership of the event from the English Department to the Maths department, the user needs *Delete Event Detail* rights for English, and *Create Event Detail* rights for Maths – it is as though the event detail is being deleted from one department and created in another. No *Modify Timetable* rights are required in this case because no changes are being made to the event resources.

- To delete an event, the user needs *Delete Event Details* rights (to delete the detail of the event) and *Modify Timetable* rights for every resource allocated to the event.
- To suspend an event, or modify its day, times or weeks, the user needs *Modify Event Detail* rights (because the detail of the record is being changed), and also *Modify Timetable* for every resource attached to the event (as changes to temporal elements effectively alter the timetable for all of the event's resources).
- To protect an event, or modify its Category, Notes, Tags, Requirements, etc, the user needs only the *Modify Event Details* right.

Departments are Special

Since access rights can be founded upon departments (see the *By Department* level above), they are handled very carefully by *Timetabler* security. Here are the situations in which departments receive special treatment:

Changing a Record's Department

Modifying a resource's department (from department X to department Y) is conceptually seen as deleting the resource altogether and re-creating it in department Y. This makes it possible for a user to have *Modify Record* rights to two or more departments without fear of them transferring resources from one department to another.

Adding Departments

Creation of a new department requires the *Create Record* (C) rights for departments. When the user creates a department they will automatically receive full access rights to *All Records* (A) in that department (via the *By Department* permission level).

Creating Events

In order to create an event, a user needs *Create Event Detail* rights. This may be provided using a *By Department* level, in which case the user must specify an appropriate department when creating the event or they will be unable to save it.

Default Access Rights

What access rights apply in a newly-created timetable? Understandably, there are no *By Department* or *By Item* rights at this stage because there are no departments or resources in the timetable database. Furthermore, there are not yet any *By Type* access rights established. Referring back to the permission levels hierarchy reveals that the *By Timetable* access rights prevail in this situation – a set of default access rights that are created along with every timetable. You can examine and modify these timetable-wide access rights in the Settings page of the CELCAT *Timetabler* Administrator application. The default rights are *View* (V) for everything except *Event Details* (to which *All* (A) access is given).

At this point only the built-in Administrator account can be used to create records in the database. N.B. A user with an Administrative role has unrestricted access to all parts of the timetable – access rights are ignored.

You should modify the default rights in the Settings page of CELCAT *Timetabler* Administrator in order to provide sensible default access rights for your institution.

Once this is done you can then override these for specific roles using the *By Type*, *By Department* and *By Item* permission levels.

Note – It is good practice to modify the default Administrator name and password and to create a backup administrative account.

Protected Fields

As an extension to the access rights mechanism, *Timetabler* also provides a means of protecting individual record fields. This is configured on a per-role basis and is maintained by the *Timetabler* Administrator application (see the *Roles* page, *Protected Fields* tab).

Protect attributes prevent individual fields of a record from being edited. They are applied to all records and they do not prevent the attributes from being viewed, nor do they protect the record itself from being deleted. However, when applied, they take precedence over all access right. There are no permission levels in the *Protected Fields* mechanism (such as protection by department or by type); a user cannot modify the value of a protected field in any record. In the user interface of *Timetabler* applications, protected fields are sometimes greyed out to indicate they cannot be edited.

Do not confuse the *Protected Fields* mechanism described above with the ability to ‘protect’ an event in the *Timetabler* event window. This latter function is used simply to denote a special event status and has no relationship to access rights.

SAT Extended Absence Rights

CELCAT Student Attendance software (SAT) is used to record student attendance on registers. A prerequisite for any use of SAT functions is that the user has the special “May use SAT” attribute set in *Timetabler* Administrator.

Access to *Extended Absence* records for a particular student is determined by a user’s access rights for the Student Record. The *Modify* (M) attribute is required in order to edit, create or remove extended absence records.

The Deny (X) attribute would prevent a user viewing the list of extended absences for a given student. However, individual occurrences of an extended absence can still be viewed in a register or SAT report for which the user has *View* access.

Access Rights and Printing

Access rights required for printing reports are similar to those required to view data on screen. Details are as follows:

Grid and List Timetables

The user requires *View Timetable* rights to select the resources to print.

Statistics

The user requires *View Statistics* rights to select resources to print.

SAT Register Reports

The user requires *View Register* rights for at least one member of staff assigned to the register when selecting registers to print. The two exceptions are for registers with no members of staff assigned (which are printable by all users), and a user’s own registers.

SAT Departmental Reports

The user requires *View Attendance* rights for each event included in the report.

SAT Resource Reports

The user requires *View Statistics* rights to select resources to print.

Web Publishing Timetables

The user requires *View Timetable* rights to select resources to publish.



Rev 1.5 Jan 2007

Copyright © 2005, 2007 CELCAT