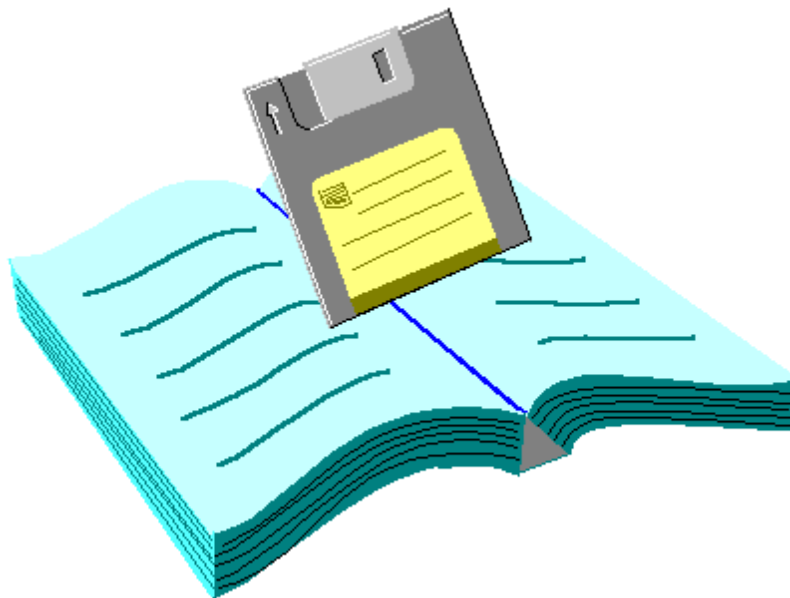


Velos Security Administrator Manual

Version 4.0



Updated December 2007

TABLE OF CONTENTS

SECTION 1: VELOS SECURITY	1-1
1.1 OVERVIEW.....	1-2
1.2 TYPES OF USERS.....	1-2
1.3 USER GROUPS.....	1-2
1.4 SECURITY LEVELS	1-3
1.4.1 Types of Security.....	1-3
1.4.2 Facility-Based Security.....	1-3
1.4.3 Operational Level Security.....	1-3
1.4.4 Control Level Security.....	1-4
1.5 SECURITY NAVIGATION.....	1-4
1.5.1 Security Browser	1-4
1.5.2 How to Create a User.....	1-6
1.5.3 How to Create a Group	1-8
1.5.4 How to Define Module Level Security	1-9
1.5.5 How to Define Control Level Security.....	1-10
1.5.6 Making Fields Mandatory	1-12
1.6 FREQUENTLY ASKED QUESTIONS	1-13
1.6.1 If a user is a member of a group with access rights that are different than his/her individual rights settings, which settings take precedence?	1-13
1.6.2 What if a user forgets their password?	1-13
1.7 TROUBLESHOOTING.....	1-13
1.7.1 Security is Disabled.....	1-13
1.7.2 Security Not Working.....	1-14

TABLE OF FIGURES

FIGURE 1.1: SECURITY MENU	5
FIGURE 1.2: LIST OF VELOS USERS	5
FIGURE 1.3: NEW USER ACCOUNT	7
FIGURE 1.4: GROUP CREATION.....	8
FIGURE 1.5: MODULE LEVEL SECURITY.....	9
FIGURE 1.6: CONTROL LEVEL SECURITY.....	10
FIGURE 1.7: EXAMPLES OF CONTROLS ON MEDICATION BROWSER	11
FIGURE 1.8: MAINTENANCE SCREEN FOR MANDATORY FIELDS.....	12



ABOUT THIS MANUAL

Outline

This operations manual is an in-depth guide designed to provide adequate training to the end users of Velos products, in order for those users to perform their respective functions. The objective of the document is to enhance this learning process by writing in easy to understand terms. The various printed screens of the running application are used to enhance the understanding of Velos.

Note: The reader should have a thorough understanding of each section before proceeding to the next.

Structure

This manual is divided into various sections, as listed below.

- 1.1 Overview**
- 1.2 Users**
- 1.3 User Groups**
- 1.4 Security Levels**
- 1.5 Security Navigation**
- 1.6 Frequently Asked Questions**
- 1.7 Troubleshooting**

Legends Used

Below are the definitions of various symbols/icons used in this manual, which appear throughout to emphasize some important information or instruction:



The Document Icon explains general features.



The Hand Icon is used to indicate some noticeable features, hints or things to do.



The Key Icon indicates some helpful tip or shortcut that will make a task easier.



The Bell Icon represents some important information.



The Time Bomb Icon is a warning message that alerts the user about the things not to be done to avoid errors.



The Hourglass Icon represents the end of a section.

Section 1: Velos Security

Security Administrator Manual





SECTION 1: VELOS SECURITY

1.1 Overview

Velos is a multi-user application with users of all levels accessing its database. In order to protect the database from being corrupted or misused, the Velos system has a **Security** feature that allows only a few trusted users to manage the system. The security system needs to restrict the domain for each user. A user in Velos is allocated access rights, which decide how far a user can enter the system. These access rights can give a user full control over the system, in which case the user is called an ‘Administrator,’ or they can be restricted heavily, in which case the user is called a ‘Guest’. In between these two states of access rights, there are numerous combinations of access rights that can be assigned to the user as the situation demands.

The assignment of these rights decides the type of data the user will be able to view, modify, delete, and so forth. Thus, by limiting the access level of the users, the data can be protected and the information flow can be controlled.

1.2 Types of Users

A user is defined as anyone who uses the application. Users are also called ‘Providers’ within the system. A user can be a normal user or an administrator.

An administrator is one who creates and maintains security and user information for the system. His/her role is to create users and give them appropriate rights to use system. The administrator may be one of the providers or any other person who is authorized to control the system. Once the administrator’s account is created, the administrator creates and assigns access rights to the other users of the system. The administrator can also modify and delete the profiles of other users, as well as form groups to include all users who share the same security settings.

All users in Velos who do not have administrative privileges are considered normal users. They may or may not be given rights to view, modify, or delete information on any given screen, as appropriate to their role within the organization.

1.3 User Groups

A set of users can be grouped together. A single user can be a part of more than one group. Groups are formed to give the same access rights to all users belonging to that group. For example, all nurses may be in one group with limited rights, whereas all doctors may be placed in another group that has more access rights. This makes it easier to set the access rights of a group of users rather than setting up each account individually.

1.4 Security Levels

1.4.1 Types of Security

Velos Security can be controlled through three different types of security, based on facility, operations, and control levels. The following sections explain more about each kind of security and how to use it.

1.4.2 Facility-Based Security

This type of security is useful for the multi-facility organization where a shared Velos sever is accessed by multiple clients at various facilities. In that case, the administrator may want to restrict users to be able only to access data from the selected facility at which they work. In this type of security, the administrator assigns each user to a particular facility when the user's account is created. This will prevent users from accessing data that they are not authorized to view.

1.4.3 Operational Level Security

This security feature allows the administrator to determine which operations a user is able to perform within the Velos database. Operational level Security can be set at two levels: application level (which applies to the entire Velos system) or module level (which applies only to a certain module within Velos). There are five operations which can be allowed or disallowed for a user or user group, determining the extent to which he/she can access and change information. These operations are:

- **New:** This option controls the user's right to enter the new data. When disabled, the menu icon corresponding to this option is deactivated. As a result, the user will not be able to enter any new data into the Velos database.
- **Modify:** This option controls the user's right to modify the existing data. A user may be given the privilege to see existing data but not the ability to change it if this option is disabled for the user.
- **View:** This option controls the user's right to view the existing data. This is the most basic right and must be granted if any other rights are granted for the specified module or function.
- **Delete:** This option controls the user's right to delete the existing data. When disabled, the menu icon corresponding to this option is deactivated. As a result, the user will not be able to delete any data from the database.
- **Maintenance:** This option controls the user's right to use the maintenance functions within Velos. When disabled, the menu icon corresponding to this option is deactivated.

The use of maintenance data is different from the other data which is patient-related. When the maintenance option is enabled for a user (for an administrator or for another privileged user), any of New/Modify/View/Delete operations can be performed on maintenance data (code lists, assessments, worklists, names of medications, diagnoses, problems, etc.) irrespective of whether these rights are given for patient data or not.

Application level security is set when creating a new user or group. These rights will apply to the entire Velos application.

Module level security is defined through the Security Management feature. Module level security is used to grant or revoke specific rights to a user in some particular modules and not on the entire application. When a security setting is defined at this level for a user or group, the module level security setting overrides the application level setting in the specified module only.



The Maintenance option is not provided at module level.

1.4.4 Control Level Security

Controls are the objects that appear on the screen and through which a user interacts with the application. For example, any icon on the toolbar that you click on to perform a particular function is considered a control. In this type of security, the user's level of interaction with these controls is determined by the control being enabled, disabled, or invisible for that user. Control level security allows the administrator to hide or disable some controls for a particular user, if that is not authorized to see or modify some field value. The controls have the following states:

- *Not set:* Depicts no specific setting.
- *Enabled:* Control is visible and enabled.
- *Disabled:* Control is visible on the screen, but disabled for the user.
- *Invisible:* Control is disabled and invisible, or not displayed on the screen.

These settings can be adjusted using the Security Management screen.



The administrator can set the choices as required for individual users or for groups.

1.5 Security Navigation

1.5.1 Security Browser

To access security settings in Velos, the administrator must use the Security Browser. To do this, first click on **File** in the menu bar and choose **Security...**, as shown in Figure 1.1. A window titled **Security Browser** will appear. This browser screen contains two tabs: Users and Groups, where the administrator can browse through and make changes to the lists of either users and or groups.

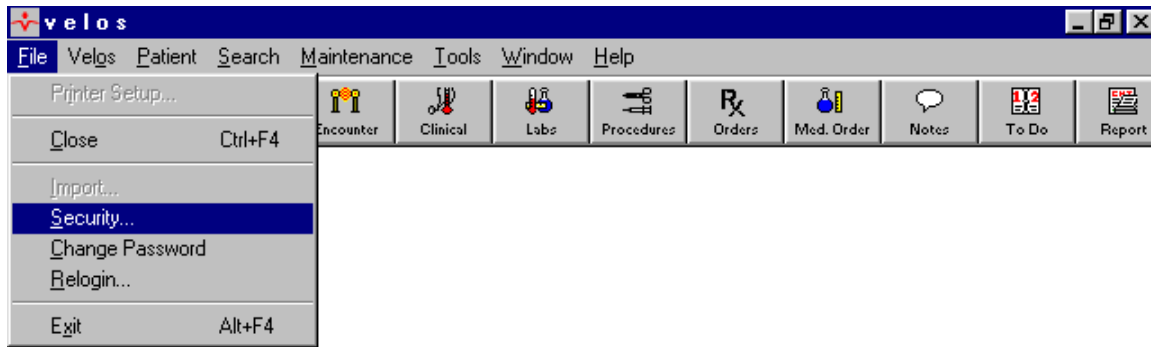



Figure 1.1: Security Menu

 *Figure 1.1 shows the **Security** option in the **File** menu. This is how the administrator can access the security settings.*

As you can see in Figure 1.2, the **Users** tab displays the list of **Provider Names** on the left side and their respective **Login Names** on the right side.

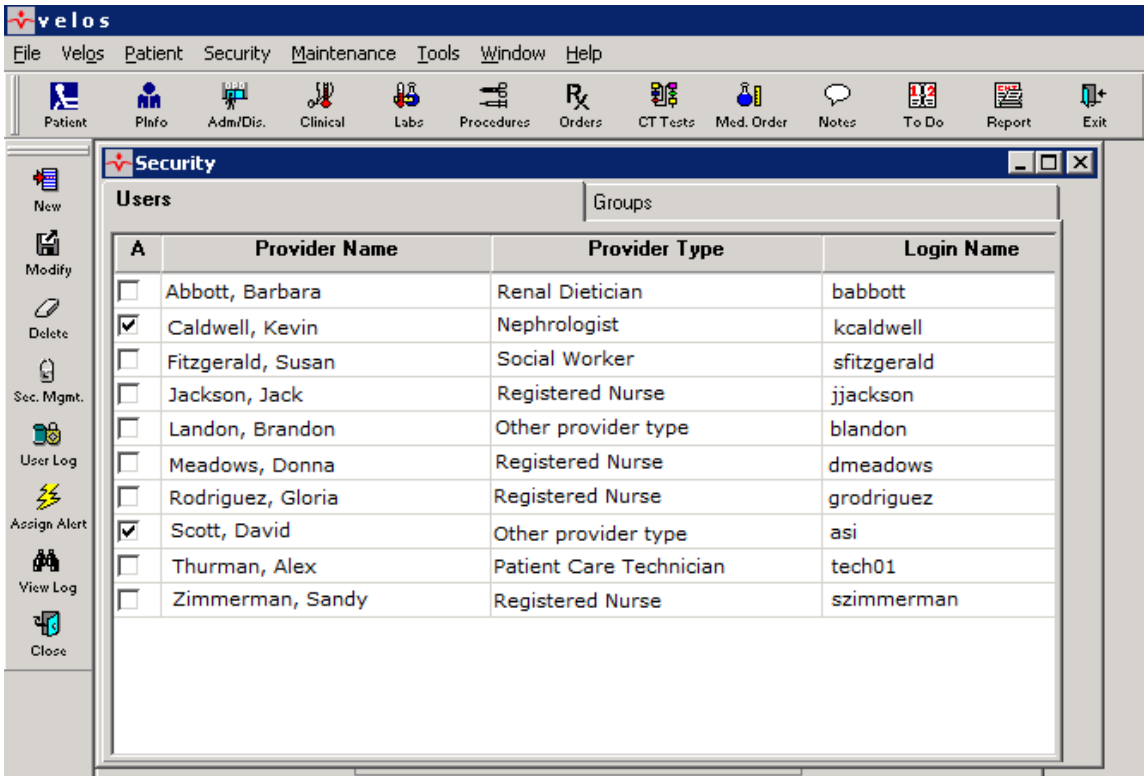


Figure 1.2: List of Velos Users



Figure 1.2 shows the **Users** tab in the **Security Browser** screen. This screen opens when you select the **Security** from the **File** menu. This screen allows creating and modifying the user accounts.

The administrator can use the following buttons, located on the left toolbar, to make changes to user settings.



Allows the administrator to add a new user or group (Refer to Figure 1.3).



Allows the administrator to modify the selected user's or group's account, including access rights, login names, passwords, and e-signatures.



Allows the administrator to delete the selected user or group from the existing list.



This button opens the Security Management feature. This will open a new window where more specific rights can be assigned to a group or user.

1.5.2 How to Create a User

To create a new user, the user must first be entered into the system as a provider. To do this, go to Provider Maintenance and add the provider. For more details on this process, see Section 4.17: Provider Maintenance in the Velos Core Operations Manual. Next, follow the steps below.

- Step 1: Click **New** while the **User** tab is selected as shown in Figure 1.2. This will open the **New User** screen shown in Figure 1.3.
- Step 2: Select the provider for whom you are going to create an account. Give this user a login name, password, and e-signature. The login name does not have to be the user's real name, but may be determined by your facility's standards or procedures. The user will be able to change their password and e-signature when they log in so that they will be confidential, but they cannot change their own login name.
- Step 3: Next, assign **New/Modify/View/Delete/Maintenance** rights to the user, as appropriate to their role in the organization, by checking or unchecking the boxes next to these words. In the example in Figure 1.3, John Philips has been given new, view, and maintenance rights but will be unable to modify or delete existing patient information.

- Step 4: Check the box next to **Administrator** if the user should be given control over security settings and other administrative rights. Leave the box unchecked if the user is a normal user.
- Step 5: Use the **Default Encounter** drop-down list to choose an encounter that will automatically be opened when the user logs on. The encounter may be changed if necessary, but if the user consistently uses one particular encounter, choosing this as his/her default encounter will save the user time and make his/her job easier.
- Step 6: For a multi-facility organization, the administrator can assign the facility or facilities for which the user can access patient data and perform the operations allowed. To do this, highlight the facility names and use the **Grant** and **Revoke** buttons to move facilities from the **All Facilities** box to the **Selected Facilities** box, or vice versa. In Figure 1.3, John Philips has access to two facilities' databases, but not to the two others whose names remain in the **All Facilities** box.

Figure 1.3: New User Account



Figure 1.3 shows the New User creation screen in **Security**. This screen opens when you select the **New** option in **Security** when the user tab is selected. This is also the screen you see when you modify an existing user's account.

Step 7: Now press **OK** to save these settings. The new user will be created and this person can now log on using the specified user name and password.



If the Login name has already been used for another user, or the password or e-signature does not match the re-entered version, you will get an error message. You cannot create the new user until you correct the error.

1.5.3 How to Create a Group

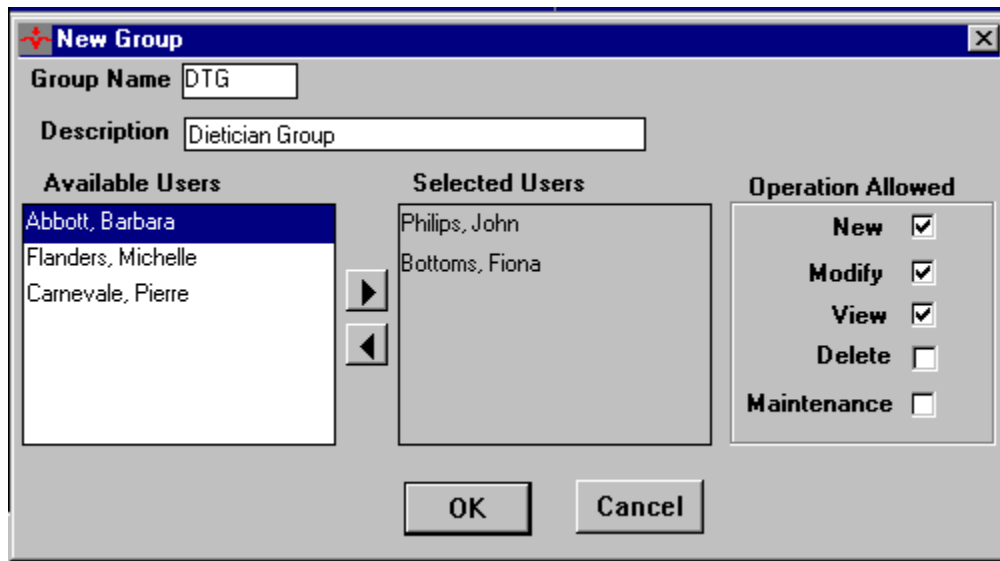


Figure 1.4: Group Creation



*Figure 1.4 shows the **New Group** window which allows the administrator to create a new group of users. This screen opens when the **Groups** tab of the **Security Browser** window is selected and the **New** button is clicked on.*

To create groups of users, follow the steps below.

Step 1: Select the **Groups** tab on the Security Browser and click **New**. This will open the **New Group** screen shown in Figure 1.4.

Step 2: Enter the group name and its description in the fields provided.

Step 3: Select the users which you want to include in the new group. Highlight them and use the arrows to move them from the **Available Users** box to the **Selected Users** box.

Step 4: Define the **Operations Allowed** for that group.

Step 5: Click **OK** to save the group information. All the users belonging to this group will automatically have the rights defined for the group.

1.5.4 How to Define Module Level Security

To define security at module level, follow the steps below.

- Step 1: Select a user or a group from the Security Browser and click the **Sec. Mgmt.** icon on the left toolbar. This will open the **Security Management** screen, shown in Figure 1.5. The drop-down menu will be pre-populated with the selected user or group.
- Step 2: Here you will see the application's modules depicted in a hierarchical tree structure on the left of the window. Each folder represents a module in Velos.
- Step 3: Select a module for which you want to override the settings defined at application level for the selected user or group. This will give them different security rights in that particular module only. Click on the module to highlight it.
- Step 4: When a module is selected, by default the window will show the rights defined at application level for that user or group. The administrator can check or uncheck the boxes relating to the New/Modify/View/Delete privileges. For example, in Figure 1.5, John Philips has Modify and View rights in the Med Order module. This will apply to the selected module and any sub-modules that may exist within it.
- Step 5: Click **Save**. You may also make changes in additional modules or change the user or group selected in the drop-down menu in order to alter additional security settings. When you are done with all changes, click **Save** and then **Close**.

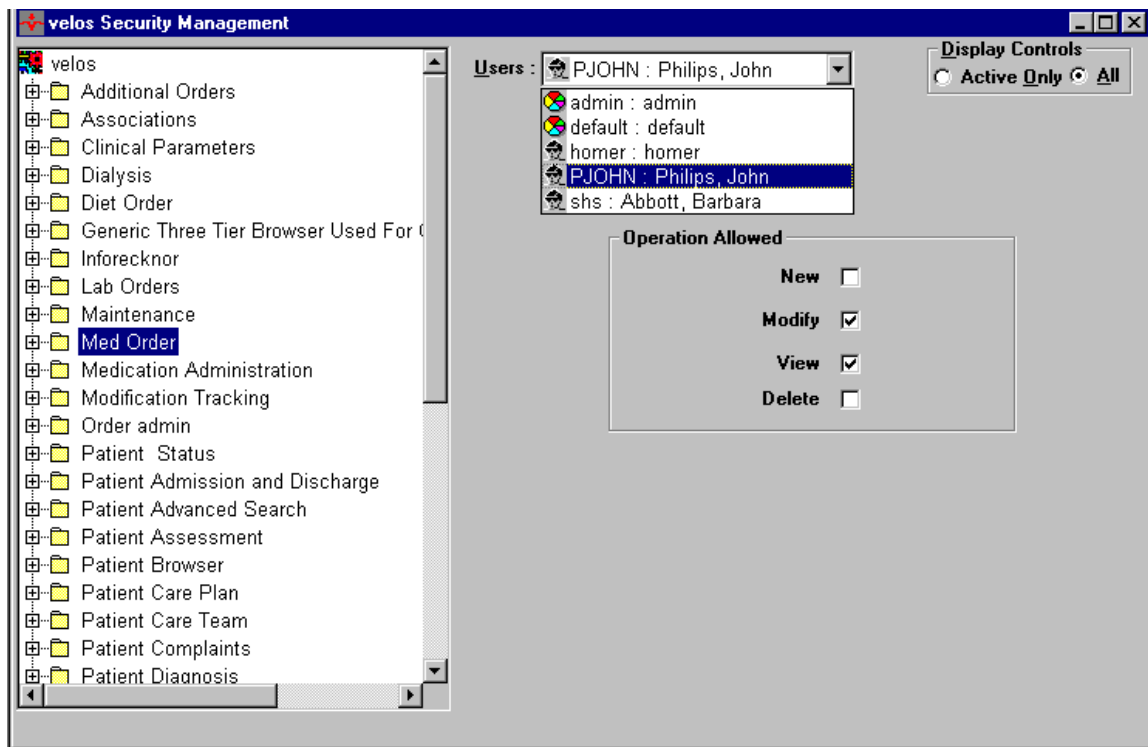


Figure 1.5: Module Level Security



Figure 1.5 shows the **Security Management** screen. This screen opens when you click the **Sec. Mgmt.** icon in the Security Browser. This screen allows the administrator to define or change module-level security.

1.5.5 How to Define Control Level Security

To define security at control level, follow the steps below.

Step 1: Select a user or a group from the Security Browser and click the **Sec. Mgmt.** icon on the left toolbar. This will open the **Security Management** screen, shown in Figures 1.5 and 1.6. The drop-down menu will be pre-populated with the selected user or group.

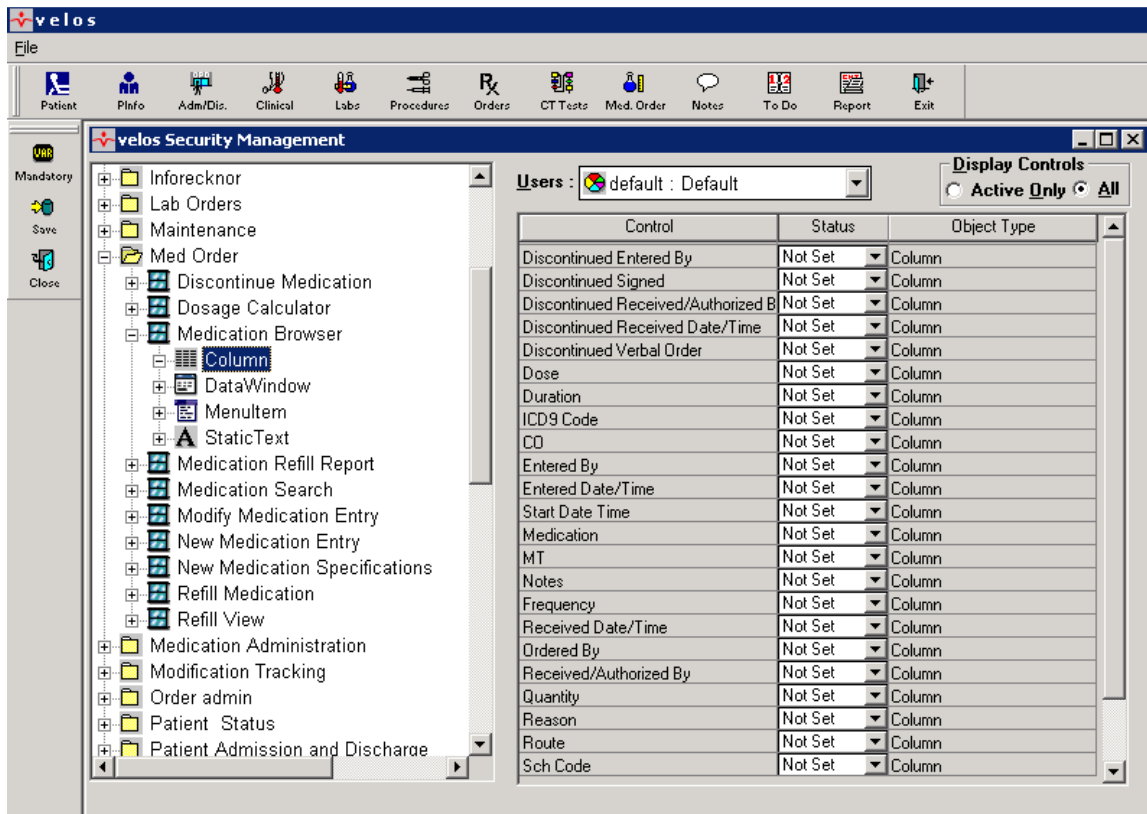


Figure 1.6: Control Level Security



Figure 1.6 shows the control level security accessed in the **Security Management** screen. This screen allows the administrator to define control level security.

Step 2: Here you will see the application's modules depicted in a hierarchical tree structure on the left of the window. Each folder represents a module in Velos. Within each folder is a list of all available screens in that module. Under each individual screen is a list of all the controls available on that screen. Figure 1.6 shows the **Med Order** module opened to show all screens, and the **Medication Browser** screen opened to show all controls for that screen. Refer to Figure 1.7 to see which parts of the Medication Browser screen each of these controls refers to.

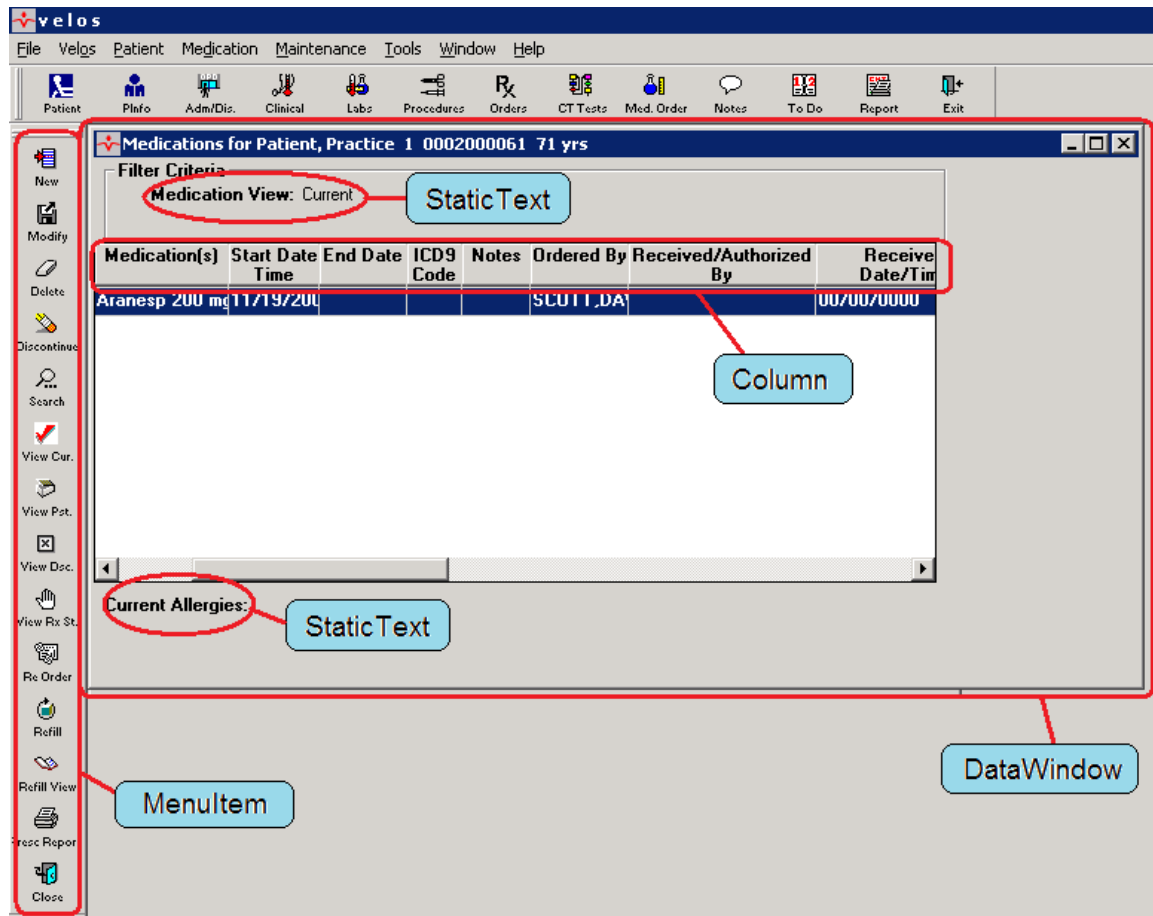


Figure 1.7: Examples of Controls on Medication Browser

Step 3: Select the type of control on a particular screen for which you want to restrict the user or group's access. You can open or close modules and screens by double-clicking on their names, or by clicking on the + or – symbol beside the icon, which shows whether they are opened or closed.

Step 4: When you select a control type in left tree window, a list of all controls of that type appears on the right side of the window, along with its current status. For example, in Figure 1.6, the **Column** control type is selected, and all controls which appear in the columns of the Medication Browser are listed on the right of the Security Management window. By default, the status of all controls will be

listed as **Not Set**. This may be changed to **Enabled**, **Disabled**, or **Invisible** using the drop-down menu.

Step 5: Select and change settings for as many controls as desired for as many groups or users as you like.

Step 6: Click **Save** and **Close** to complete your changes.

1.5.6 Making Fields Mandatory

Another function available within Security Management is the ability to make certain fields mandatory. This is helpful if certain users often forget to fill in information which later turns out to be important. Using this function will prevent users from leaving the current screen until they have filled out the fields which are set as mandatory by the administrator. Since different organizations collect different information and have various policies regarding what information is required, Velos has included this function so that administrators can customize the system to meet the standards of their particular facility or organization.

To use this function, access the Security Management browser by clicking on the **File** menu, selecting **Security...** and then clicking the **Sec. Mgmt.** icon on the left toolbar. Next, choose the **Mandatory** icon on the left toolbar of the Security Management screen. This will open the window shown in Figure 1.8.

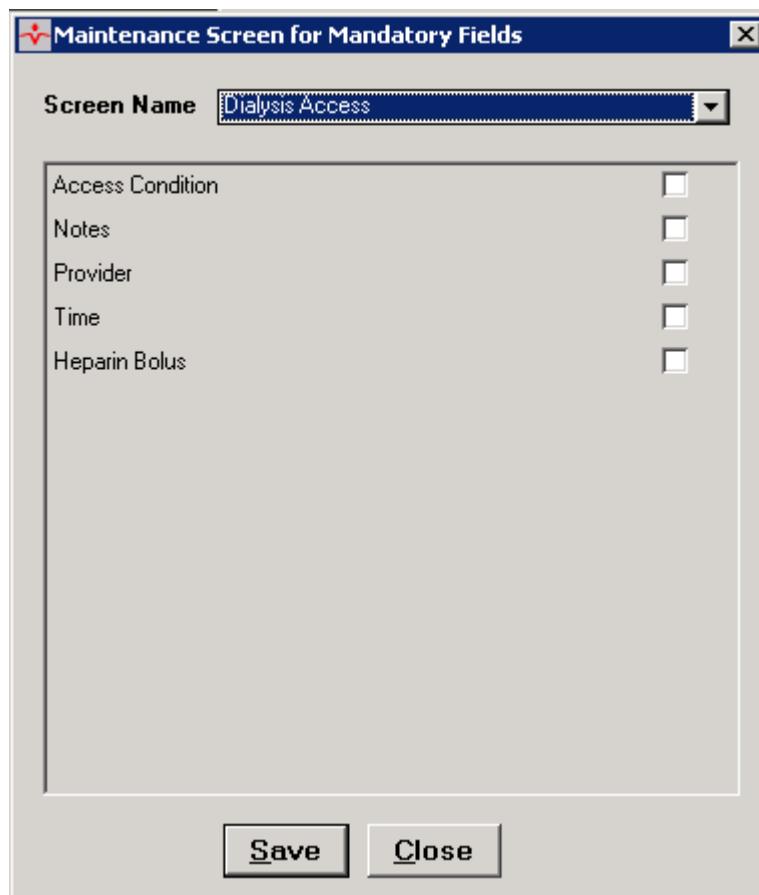


Figure 1.8: Maintenance Screen for Mandatory Fields

Here, you can select from the **Screen Name** drop-down menu the screen where you would like to make a field mandatory. Next, click the checkbox next to any field that you want to require users to fill in. Click **Save** and **Close** when you are done.

1.6 Frequently Asked Questions

This section lists some commonly-asked questions related to security and its behavior.

1.6.1 If a user is a member of a group with access rights that are different than his/her individual rights settings, which settings take precedence?

Velos is designed to provide a maximum level of security. To achieve this, it combines the individual user rights and the rights of the group(s) to which the user belongs, and then picks the minimum rights for the user.

For example, if a user is given **New**, **Modify**, **View**, **Delete** and **Maintenance** privileges individually, but they are a member of a group which only has **New** and **View** rights, they will only be able to view existing data and add new data. They will **not** be able to modify or delete information, or perform maintenance tasks. This is one reason it is important to make sure users are placed groups with rights appropriate for their role in the organization.

The same concept is used when determining control-level security. When user and group security permissions are combined and a conflicting status for a control exists, the following hierarchy is used to determine the user's access: **Invisible**, **Disabled**, **Enabled**, **Not set**. This means that the most restrictive setting will take precedence. For example, if a control is set to **Invisible** for a user and **Enabled** for the group to which that user belongs, the control will be invisible to that user.

1.6.2 What if a user forgets their password?

The administrator can modify the password of any user without entering the old password. Go to **Security** and find the user in the browser. Click **Modify**. You can now specify a new password for the user. He/she can then log in using the password you assign him/her, and later change the password to something confidential.

1.7 Troubleshooting

1.7.1 Security is Disabled

If you find the Security Management menu icon disabled and all options for New/Modify/View/Delete/Maintenance protected in the user or group creation screen, security may have been disabled. Please check the security flag in the control table, which should be set at 1 for the security to work.

1.7.2 Security Not Working

If the security flag is on in control table, but operational and/or control security is still not working on any screens, it might be due to incomplete data in some of the tables, which is prerequisite for the security to work properly. Please contact a technical support representative to resolve the problem.



End of the Section.