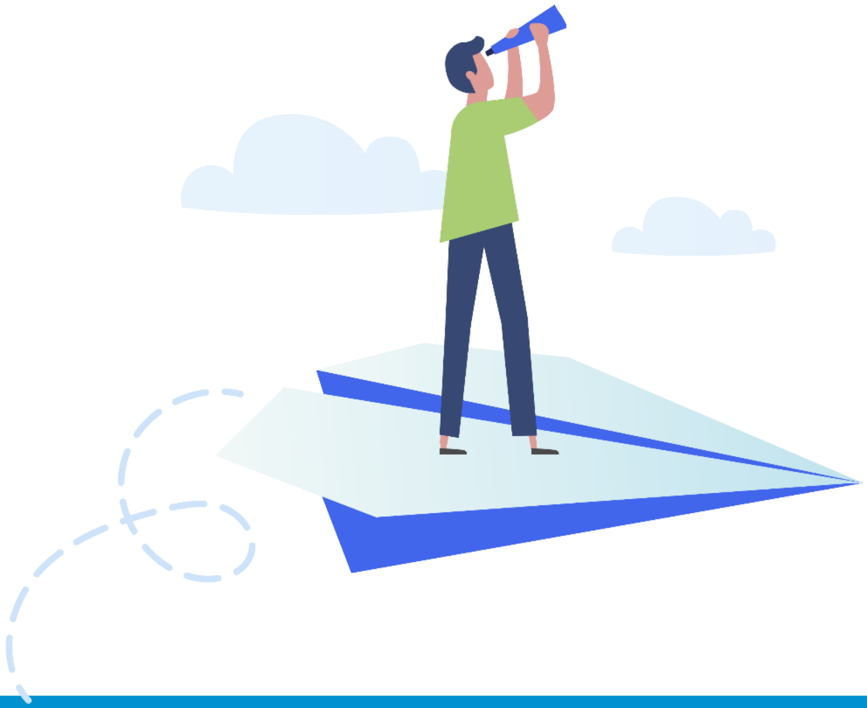
Security User Guide

Version 2

24th April 2023



No warranty of accuracy is given concerning the contents of the information contained in this publication. To the extent permitted by law, no liability (including liability to any person by reason of negligence) will be accepted by Cegedim Healthcare Solutions, its subsidiaries or employees for any direct or indirect loss or damage caused by omissions from or inaccuracies in this document.

Cegedim Healthcare Solutions reserves the right to change without notice the contents of this publication and the software to which it relates.

Product and company names herein may be the trademarks of their respective owners.

Registered name: Cegedim Rx Ltd. Registered number: 02855109
Registered name: In Practice Systems Limited. Registered number: 01788577
Registered address: Studio F5 Battersea Studios 1, 82 Silverthorne Road,
London SW8 3HE

Website: https://www.cegedim-healthcare.co.uk/

Contents

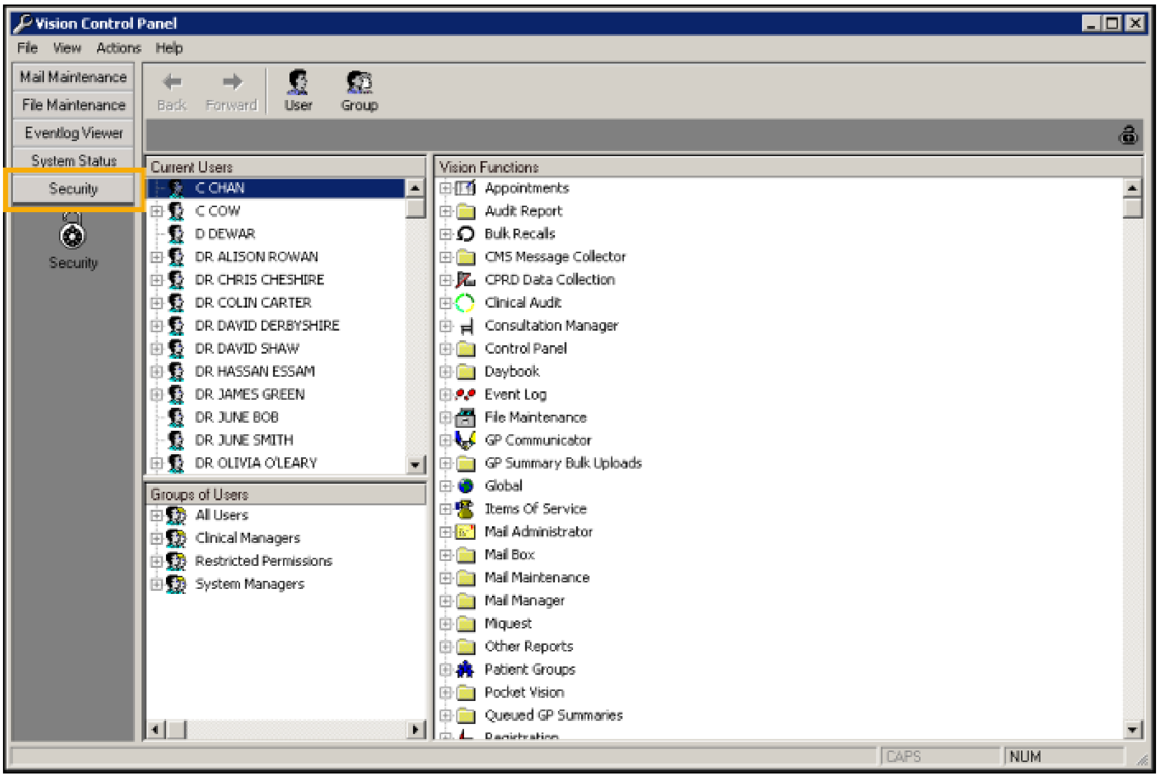
Security

Members of your practice are initially entered on to the system from **File Maintenance - Staff**. To allow them to log on to **Vision 3** they must then be added in **Security**.

Adding a staff member from **Management Tools - Control Panel - File Maintenance** automatically prompts you to add the user in **Security**.

To access **Security** directly, from the **Vision 3** front screen, select **Management Tools - Control Panel - Security**.

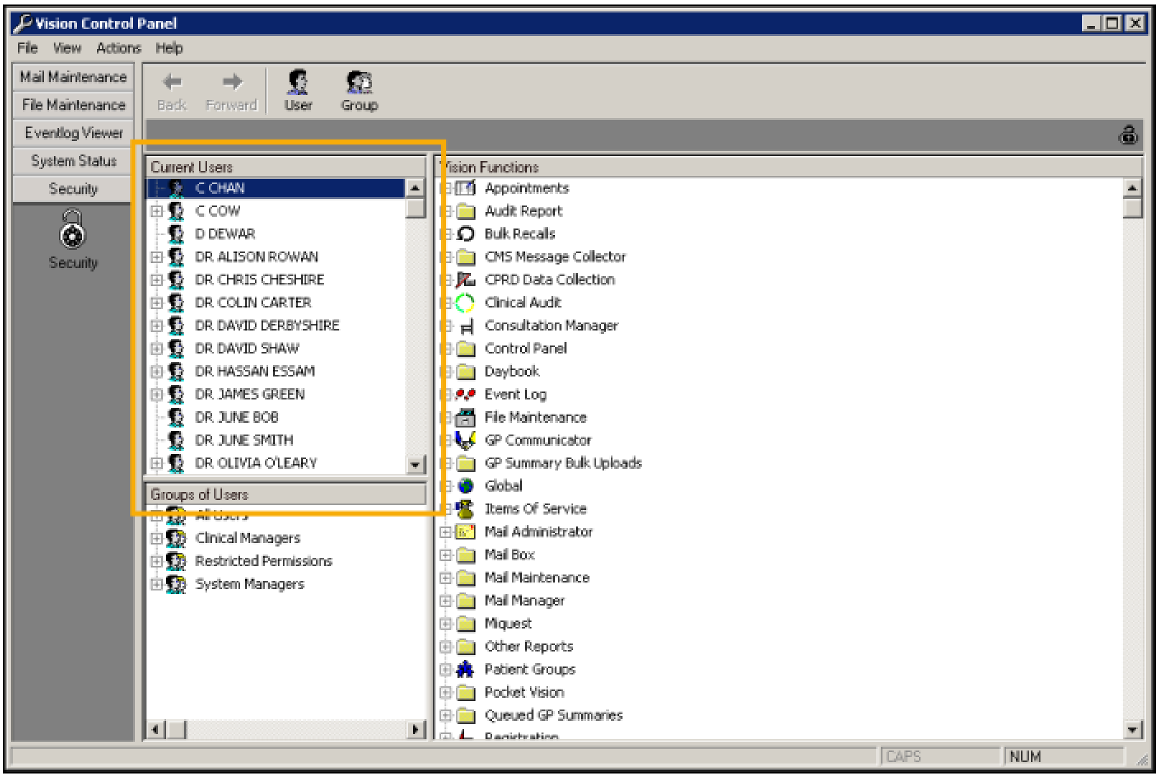
The **Security** screen is divided into three panes:



- **Current Users** (top left) - Lists all staff by their login names, see **Viewing the Current Users List** on page 5.
- **Groups of Users** (bottom left) - Staff should be added to groups with access rights to specific **Vision 3** functions, see **Security Groups** on page 15 for details.
- **Vision Functions** (right frame) - A list of modules and functions within **Vision 3**, to which individual users or groups of users can have access rights, see **Vision Functions** on page 19 for details.

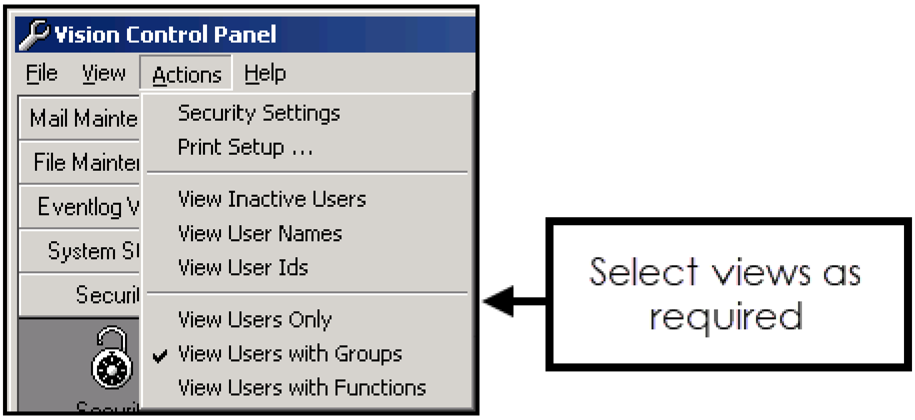
Viewing the Current Users List

Staff that have been set up in **Vision 3** display in the **Current User** section of the **Security** screen:



To define the data that displays in the panes:

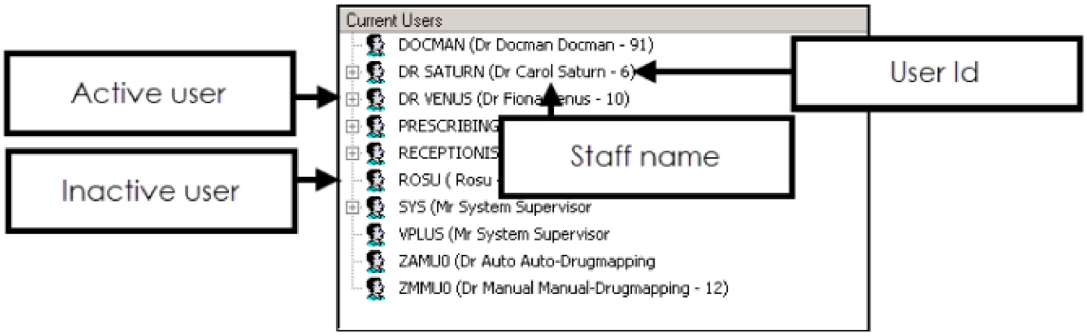
1. From the **Security** screen, select **Actions**:



Select views as required

2. Select who you want included in the list and how you want them to display, you can select one, two or all three of these option:

    - **View Inactive Users** - Ticked by default, simply untick to view current users only.
    - **View User Names** - Tick to display staff names in brackets as well as their login names.
    - **View User IDs** - Tick to display the User Ids as well as the login names:

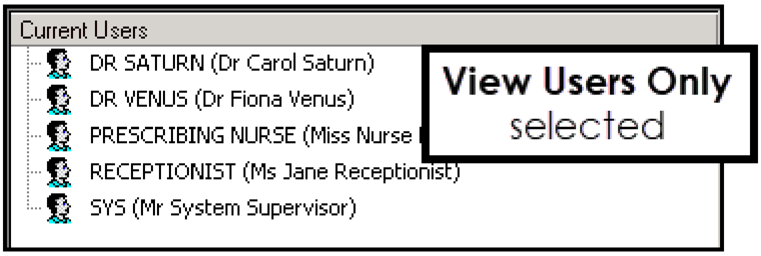


Current Users

DOCMAN (Dr Docman Docman - 91)
DR SATURN (Dr Carol Saturn - 6)
DR VENUS (Dr Fiona enus - 10)
PRESCRIBING
RECEPTIONIS
ROSU (Rosu
SYS (Mr System Supervisor
VPLUS (Mr System Supervisor
ZAMU0 (Dr Auto Auto-Drugmapping
ZMMU0 (Dr Manual Manual-Drugmapping - 12)

3. Now define what information displays for the user when you select **Expand** ⊞ next to a user's name, only one can be selected:

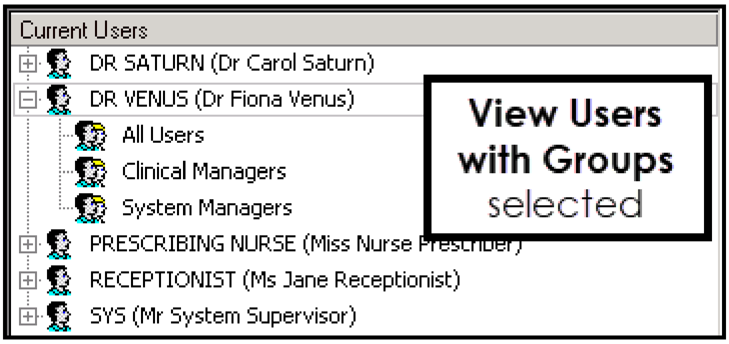
    - **View Users Only** - **Expand** ⊞ is not available, just a list of user names displays:



Current Users

DR SATURN (Dr Carol Saturn)
DR VENUS (Dr Fiona Venus)
PRESCRIBING NURSE (Miss Nurse
RECEPTIONIST (Ms Jane Receptionist)
SYS (Mr System Supervisor)

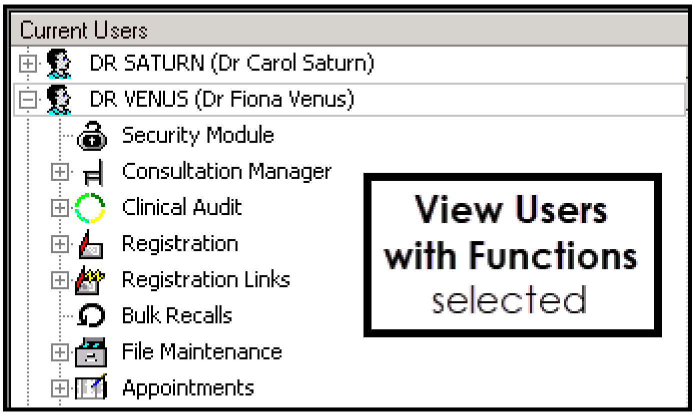
    - **View Users with Groups** - Selected by default, expanding the list beneath a user's name displays the **Security** groups they belong to, for example, All Users, System Managers and Clinical Managers:



Current Users

DR SATURN (Dr Carol Saturn)
DR VENUS (Dr Fiona Venus)
All Users
Clinical Managers
System Managers
PRESCRIBING NURSE (Miss Nurse Prescriber)
RECEPTIONIST (Ms Jane Receptionist)
SYS (Mr System Supervisor)

- **View Users with Functions** - Selecting **Expand** ⊞ lists the **Vision 3** functions they have access to:

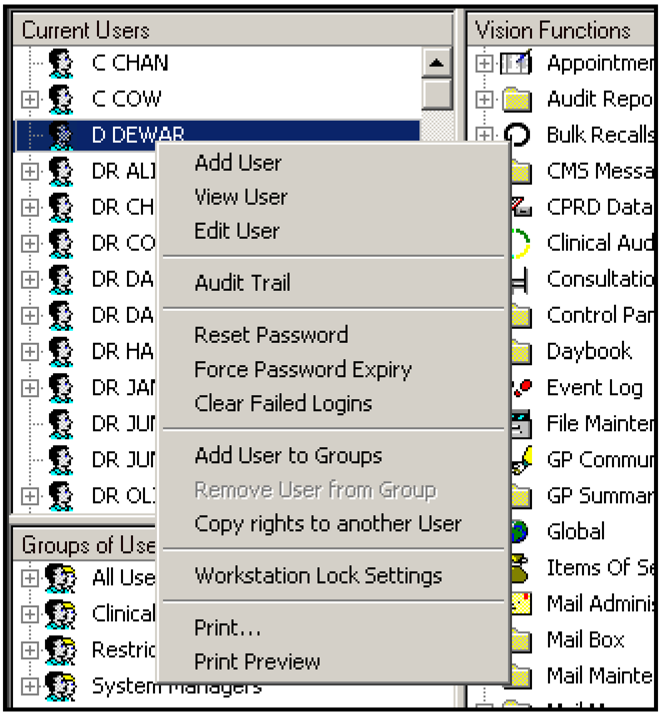


View Users with Functions selected

See **Adding or Editing Users** on page **9** for details.

Current Users - Right Click Menu

From **Management Tools** - **Control Panel** - **Security**, you can access the following options for your users. Right click on the user and select as required:



- **Add User** - Select to add a new user, see **Adding or Editing Users** on page **9** for details.
- **View User** - Select to view a user's security details.
- **Edit User** - Select to update a user's security details, see **Adding or Editing Users** on page **9** for details.
- **Audit Trail** - Select to view changes that have been made to a user's record.

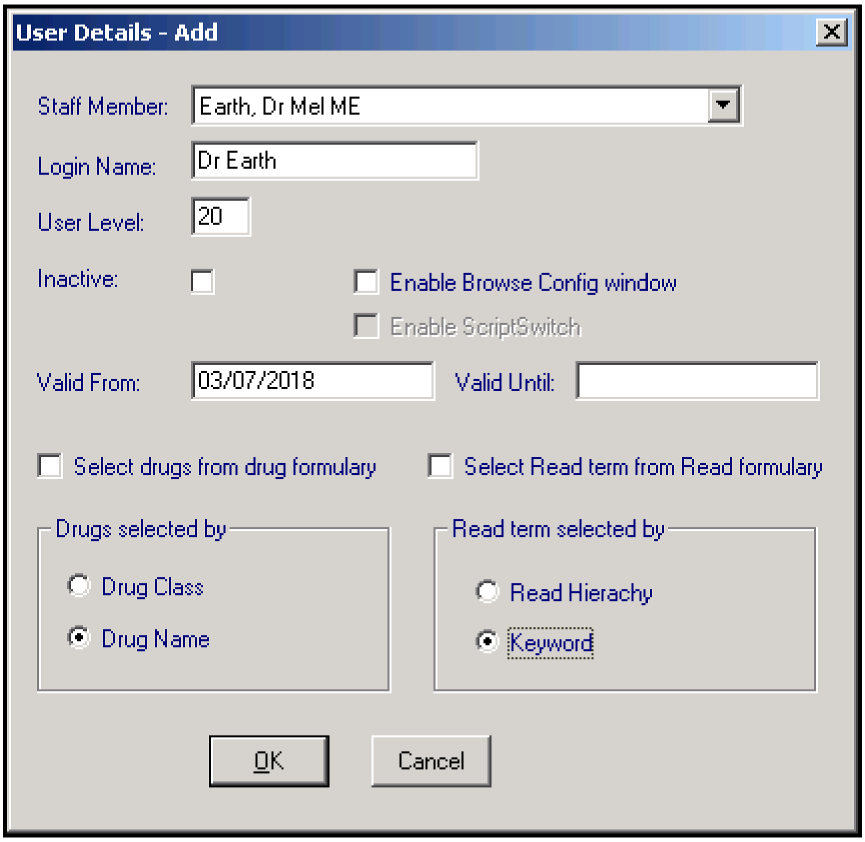
- **Reset Password** - Select to reset a user's password, see **Resetting Passwords** on page **12** for details.
- **Force Password Expiry** - Select to force a user's password to expire, for example, if they have left your employ, see **Manually Forcing a Password to Expire** on page **12** for details.
- **Clear Failed Logins** - Select to unlock the account of a user who is locked out following the accumulation of unsuccessful logins, see **Clearing Failed Logins** on page **12** for details.
- **Add User to Groups** - Select to add a user to a Security Group, see **Adding and Removing Users and Groups from Vision Functions** on page **29** for details.
- **Remove User from Group** - Select to remove a user from a Security Group, see **Adding and Removing Users and Groups from Vision Functions** on page **29** for details.
- **Copy rights to another User** - Select to copy the security and access of right of one user to another, see **Copy Rights to Another User** on page **31** for details.
- **Workstation Lock Settings** - Select to access the workstation lock settings. The user must re-enter their password to access **Vision 3** if their workstation locks. The default settings are:
    - **England** - 20 minutes
    - **Scotland** - 10 minutes
- **Print** - Select to print a list of users together with either their Security Groups or Vision Functions, depending on what is selected in **Actions** - **View Users with Groups** or **View Users with Functions**, see **Printing Security Groups and Function Rights** on page **17** for details.
- **Print Preview** - A preview of the user list, see **Printing Security Groups and Function Rights** on page **17** for details.

Adding or Editing Users

If new users are added from **Management Tools** - **Control Panel** - **File Maintenance** - **Staff**, then you are prompted to set up a user profile in **Security**.

To add or edit a staff member's security settings:

1. From **Management Tools**, select **Control Panel** Control Panel - **Security**:
   - To add a user, select **User** User from the toolbar, or right click anywhere in **Current Users** and select **Add User**.
   - To edit an existing user, select the user in **Current Users**, right click and select **Edit User**.
2. The **User Details - Add** or **- Update** screen displays:



User Details - Add

Staff Member: Earth, Dr Mel ME

Login Name: Dr Earth

User Level: 20

Inactive: □

□ Enable Browse Config window

□ Enable ScriptSwitch

Valid From: 03/07/2018

Valid Until:

□ Select drugs from drug formulary

□ Select Read term from Read formulary

Drugs selected by
○ Drug Class
● Drug Name

Read term selected by
○ Read Hierachy
● Keyword

Complete or update as required:

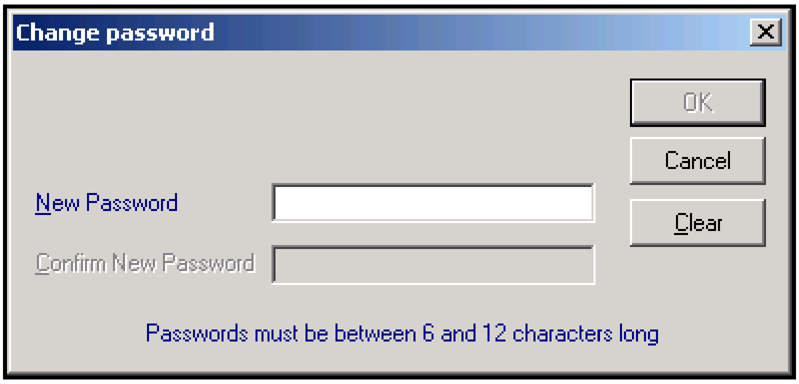
- **Staff Member** - If this is a new user, select the staff member from the available list, if you are updating a user, the correct name displays.
- **Login Name** - Add or update a log in name for your user, up to 20 characters. This is usually a reflection of their name, for example, Dr A Brown, Jane S, Nurse Amanda.
- **User Level** - This is not currently in use.
- **Inactive** - Tick if the staff member is no longer active.
- **Enable Browse Config window** - Tick to allow the user to add or remove columns on the **Select Patient** screen, recommended for system managers only.
- **Enable ScriptSwitch** - Tick to enable ScriptSwitch on an individual basis, as long as it is already switched on for the practice as a whole.

Training Tip - Scriptswitch offers specific prescribing recommendations. If a match is found, based on drug formulation, strength, dosage and therapy type, ScriptSwitch alerts the clinician at the point of prescribing. This enables clinicians to benefit from local prescribing advice at every consultation.

- **Valid From** and **Valid Until** - **Valid From** populates with today's date, leave **Valid Until** blank, but once a person has left the practice, enter the date they leave.
- **Select drugs from drug formulary** - Tick to display the drug formulary by default when selecting a drug in **Consultation Manager**. You can switch away from the formulary at the time of selection in **Therapy**:
    - **Drug selected by** - Select the way the drug dictionary displays, either by **Drug Class**, or alphabetically by **Drug Name**. Whichever is chosen becomes the default display for the user when selecting therapy items. However, it is possible to switch between the two at the time of selection.

- **Select Read term from Read formulary** - Tick to display the Read formulary by default when selecting a Read code in **Consultation Manager**. You can switch away from the formulary at the time of selection.
    - **Read term selected by** - Select either **Read Hierarchy**, the codes themselves, or **Keyword** as the default way this user selects items from the **Read Dictionary**. You can switch between the two at the time of selection.

3. Select **OK** to save.
4. For a new user, the **Change Password** screen displays:



Change password

New Password

Confirm New Password

Passwords must be between 6 and 12 characters long

Complete as follows:

- **New Password** - Enter a password, between six and twelve characters long. At least one character must be non-alphabetic. For security purposes, nothing displays on screen as you type, not even asterisks. Press the **Tab** key on your keyboard to move on.
- **Confirm New Password** - Re-enter the password in exactly the same way. A warning message displays if you have not included at least one number, or the **Confirm New Password** entry does not match the **New Password** entry.

Note - Every user needs a password to sign on to **Vision 3**, this initial password must be changed the first time the user logs on.

Important - When changing passwords, a password cannot be repeated until five other dissimilar passwords have been used.

5. Select **OK** to save.

Further options with regards passwords are explained in **Security Settings** on page **13**, including the expiry interval, minimum length, a global expiry date, and number of login retries.

Resetting Passwords

To reset a user's password:

1. Log in to **Vision 3** as a system administrator.
2. From the **Vision 3** front screen, select **Management Tools** - **Control Panel**.
3. Now select **Security**, right click on the user concerned and select **Reset Password**.
4. Enter and confirm a new password.
5. Select **OK** to save.
6. Tell the user the password you have set up.

> **Note** - The first time the user logs in they are prompted to set a new password and this one expires.

Manually Forcing a Password to Expire

To force a password to expire:

1. Log in to **Vision 3** as a system manager.
2. From the **Vision 3** front screen, select **Management Tools** - **Control Panel** - **Security**.
3. From the **Current User** list, right click on the user required and select **Force Password Expiry**.

The next time that member of staff logs in, they are forced to set a new password.

Clearing Failed Logins

You can set **Vision 3** to lock out a user if they unsuccessfully log in too many times, see Security Settings on page 13 **for details.**

To unlock a locked account:

> **Note** - You must be logged in as a System Administrator to access **Security**

1. From the **Vision 3** front screen, select **Management Tools - Control Panel** - **Security**.
2. Under **Current Users**, right click on the member of staff concerned and select **Clear Failed Logins**.

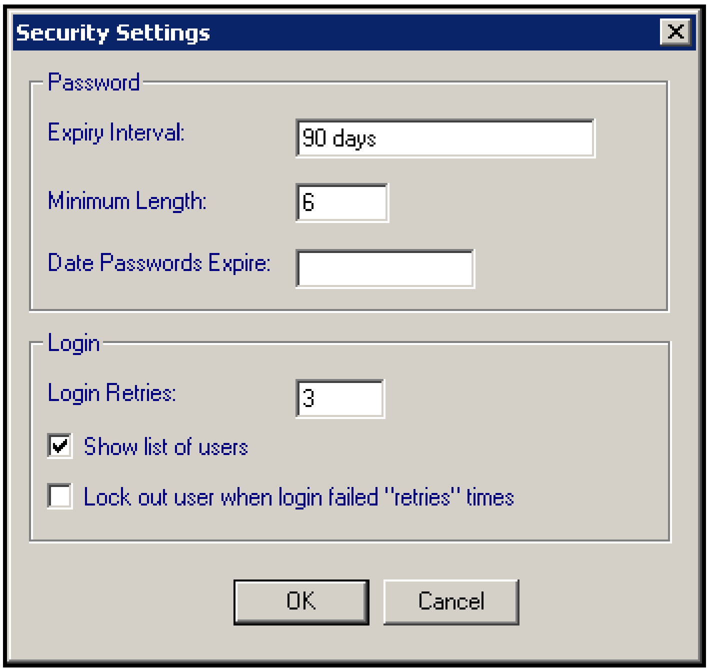
The member of staff can now log in.

Note - If the administrator is locked out contact the Help Line.

Security Settings

To update **Password** and **Login** security settings for all users:

1. From **Management Tools** - **Control Panel** - **Security**, select **Actions - Security Settings.**
2. The **Security Settings** screen displays:



Security Settings

Password

Expiry Interval: 90 days

Minimum Length: 6

Date Passwords Expire:

Login

Login Retries: 3

☑ Show list of users

□ Lock out user when login failed "retries" times

Complete as follows:

- **Expiry Interval** - Set an interval for passwords to expire, between:
    - 30 and 90 days in England, Wales and Northern Ireland.
    - 90 days in Scotland.

  Enter the expiry interval as *30D* (30 days) or *90D* (90 days).
- **Minimum Length** - Set the minimum length required for the password. **Vision 3** permits a password between 6 and 12 characters.
- **Date Passwords Expire** - Sets a global date for password expiry. This can be useful in the event of a security violation. Passwords created before the date entered expire on this date and staff are forced to create a new password before accessing the system.
- **Login Retries** - The number of times a user may attempt to login before the login process is suspended. By default, this is set to 3. The minimum is 1 and the maximum is 99.
- **Lock out user when login failed "retries" times** - Tick to retain the number of failed attempts and lock the staff member out if they exceed the **Login Retries**. Only a System Administrator can then clear failed log ins. See **Clearing Failed Logins** on page **12** for details.

> **Note** - All users can be logged out by this method, so it is important that more than one user has access to the **Security** module, so that they can unlock the other user when they are locked out.

3. Select **OK** to save.

Security Groups

Security Groups display in the bottom left pane of the **Security** screen. A security group is a collection of users to whom you wish to assign the same security rights. Both groups and individual users can be assigned to functions to grant them permission to use parts of the system. You can create your own groups, for example, *Practice Nurses* or *Receptionists*.

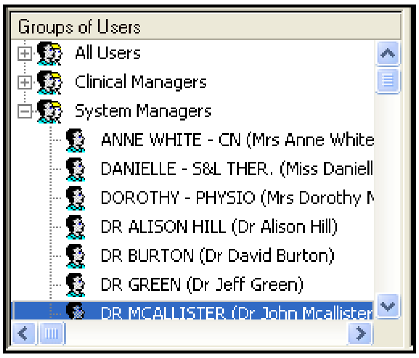
By default, users are initially grouped into three groups:

- **All Users**
- **Clinical Managers**, allowed access to clinical data (in **Consultation Manager**).
- **System Managers**, allowed access to system data, for example, **Security** and **File Maintenance**.

If a staff member has more than one user profile, each profile can be added to a different group, for example, one to **System Managers** and one to **Clinical Managers**.

> **Note** - Do not mix up **Security Group**s set up in **Security** and Staff Groups set up in **File Maintenance**. **Staff Groups** group staff for the purposes of receiving and/or actioning messages within **Mail Manager**.

In the **Groups of Users** list, select **Expand** ⊞ beside a group name, to display the staff assigned to that group, select **Collapse** ⊟ to close the list:



Groups of Users
- ⊞ All Users
- ⊞ Clinical Managers
- ⊟ System Managers
  - ANNE WHITE - CN (Mrs Anne White
  - DANIELLE - S&L THER. (Miss Daniell
  - DOROTHY - PHYSIO (Mrs Dorothy M
  - DR ALISON HILL (Dr Alison Hill)
  - DR BURTON (Dr David Burton)
  - DR GREEN (Dr Jeff Green)
  - DR MCALLISTER (Dr John Mcallister

Select a group in the bottom left pane and then right click on it to display the following options:

- **Add User(s) to Group** - Add a user from the list of users to the group selected, see **Adding and Removing Users and Groups from Vision Functions** on page **29** for details.
- **Remove User from Group** - Select **Expand** ⊞ and then right click and select **Remove User from Group** to remove a member of staff from a group.

- **Add Group** - Select to create a new group, see Adding a New Security Group on page 16 for details.
- **Edit Group** - For practice-defined groups only, select to update the description of a group.

> **Note** - You cannot edit the descriptions for the **All Users**, **Clinical Managers** or **System Manager** groups.

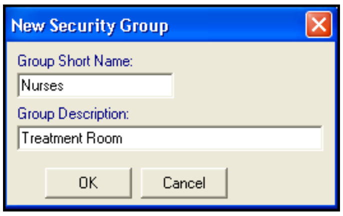
- **Delete Group** - Select to remove a group.
- **Print** - Select to print a list of users in each group.
- **Print Preview** - Select to display a preview of the list of users.

Adding a New Security Group

As a practice, you might want to define your own **Security Group** to which you can then assign common security rights. For example, the group could consist of practice nurses, or receptionists.

To create a new **Security Group**:

1. From the **Vision 3** front screen, select **Management Tools** - **Control Panel** - **Security**.
2. Select either:
    - **Group** Group from the toolbar, or
    - From **Groups of Users** in the bottom left pane, right click on one of the existing groups and select **Add Group**.
3. The New **Security Group** screen displays:



New Security Group

Group Short Name: Nurses

Group Description: Treatment Room

Complete as follows:

    - **Group Short Name** - Enter a short name for the group, 17 characters maximum, 3 characters minimum, for example, *Nurses*.
    - **Group Description** - Enter a description which must be at least four characters in length.
4. Select **OK** to save.

Your new group now displays under **Groups of Users** ready to be allocated to the appropriate **Vision Functions**.

See **Adding and Removing Users and Groups from Vision Functions** on page **29** for details.

To update the name or description of a group, simply right click on the group and select **Edit Group**.

Deleting a Security Group

To delete a security group:

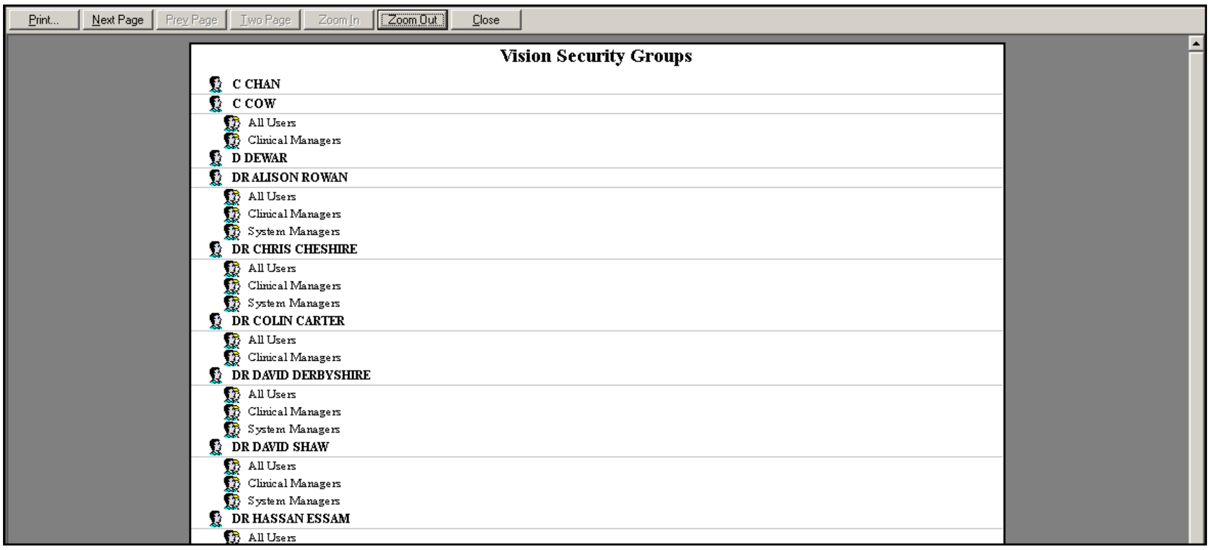
1. From the **Vision 3** front screen, select **Management Tools** - **Control Panel** - **Security**.
2. Right click on the security group no longer required and select **Delete Group.**

Note - It is not possible to delete **System Managers**, **Clinical Managers** or **All Users** groups.

Printing Security Groups and Function Rights

From **Management Tools** - **Control Panel** - **Security**, you can print the following:

- **Vision Security Groups** - You can print a list of current users and which groups they belong to. Right click within **Current Users** or the **Groups of Users** pane, select **Print Preview** and then **Print**.
- **Vision Function Rights** - You can print a list of the current access to **Vision Functions**. Right click within the **Vision Functions** pane, select **Print Preview** and then **Print**:

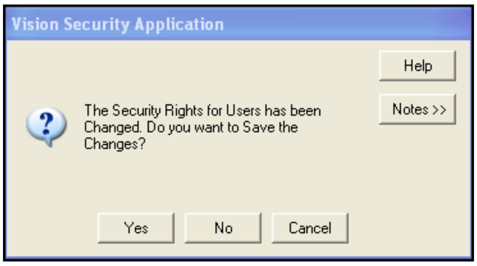


Vision Security Groups

C CHAN
C COW
All Users
Clinical Managers
D DEWAR
DR ALISON ROWAN
All Users
Clinical Managers
System Managers
DR CHRIS CHESHIRE
All Users
Clinical Managers
System Managers
DR COLIN CARTER
All Users
Clinical Managers
DR DAVID DERBYSHIRE
All Users
Clinical Managers
System Managers
DR DAVID SHAW
All Users
Clinical Managers
System Managers
DR HASSAN ESSAM
All Users

Saving and Exiting from Security

Before exiting **Security** or switching to another module, if you have made any changes involving the access of a member of staff, a Vision function, or the addition or removal of a user from a group, a '*The Security Rights for Users has been Changed. Do you want to Save the Changes? Yes/No*' warning displays:



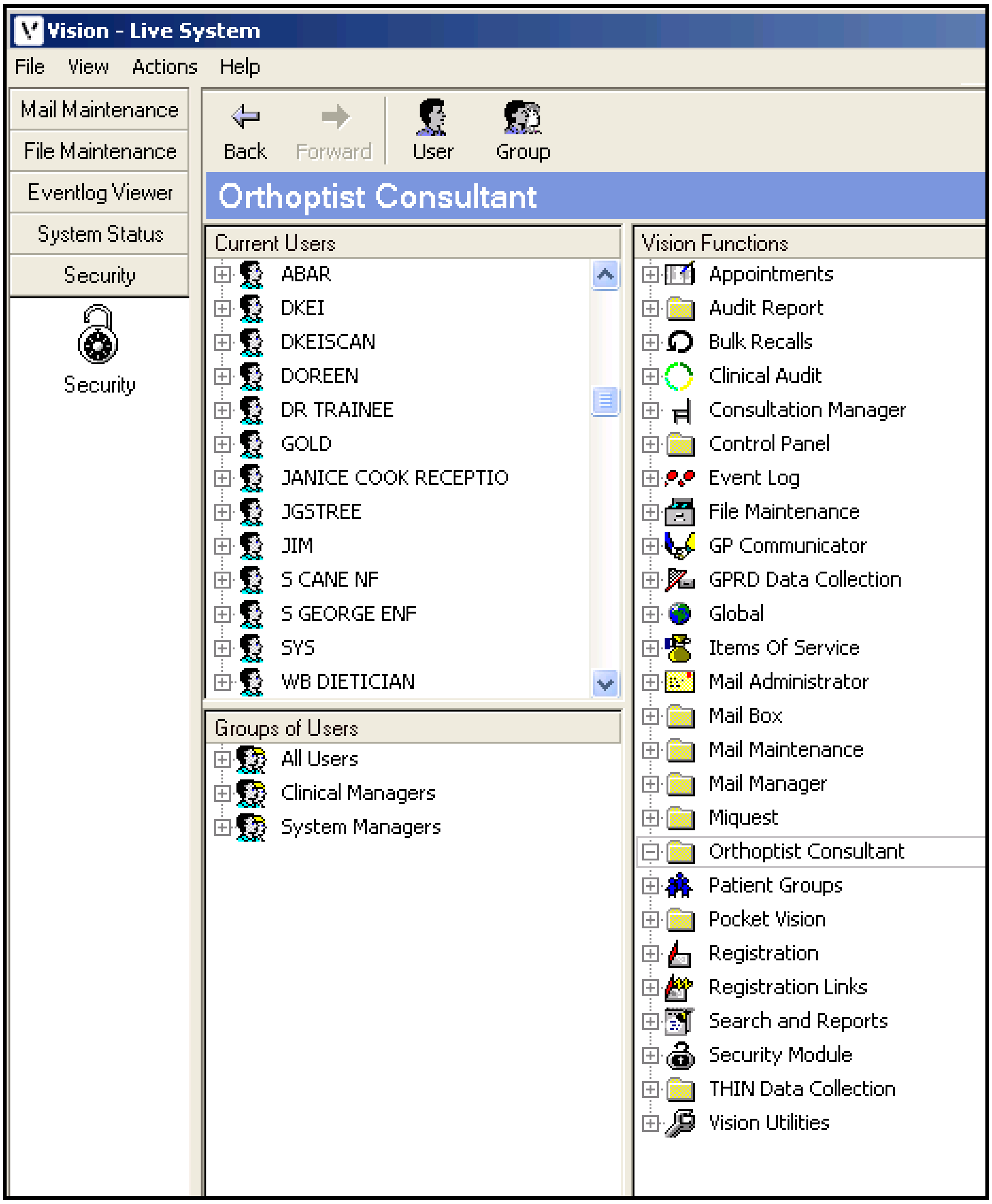
The Security Rights for Users has been Changed. Do you want to Save the Changes?

Select:

- **Yes** to save changes,
- **No** to exit without saving your changes, or
- **Cancel** to return to the **Security** screen.

Vision Functions

From **Management Tools** - **Control Panel** - **Security**, the right-hand section of the screen lists all **Vision 3** functions. This is where you determine which users have access to which functions:



Vision - Live System

File View Actions Help

Mail Maintenance
File Maintenance
Eventlog Viewer
System Status
Security

Security

Back Forward User Group

Orthoptist Consultant

Current Users

- ABAR
- DKEI
- DKEISCAN
- DOREEN
- DR TRAINEE
- GOLD
- JANICE COOK RECEPTIO
- JGSTREE
- JIM
- S CANE NF
- S GEORGE ENF
- SYS
- WB DIETICIAN

Groups of Users

- All Users
- Clinical Managers
- System Managers

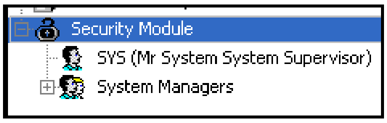
Vision Functions

- Appointments
- Audit Report
- Bulk Recalls
- Clinical Audit
- Consultation Manager
- Control Panel
- Event Log
- File Maintenance
- GP Communicator
- GPRD Data Collection
- Global
- Items Of Service
- Mail Administrator
- Mail Box
- Mail Maintenance
- Mail Manager
- Miquest
- Orthoptist Consultant
- Patient Groups
- Pocket Vision
- Registration
- Registration Links
- Search and Reports
- Security Module
- THIN Data Collection
- Vision Utilities

By default:

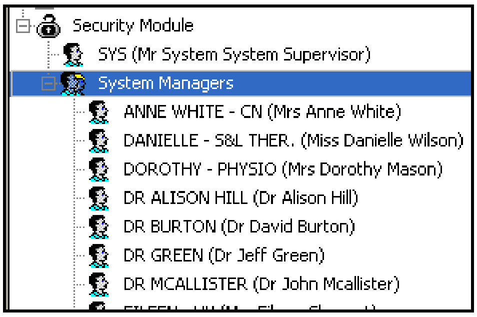
- Only System Managers have access to **Security** and **File Maintenance**.
- Only Clinical Managers have access to **Consultation Manager:**

Select **Expand** ⊞ to see which groups are currently assigned to the function, and **Collapse** ⊟ to collapse it again:



Security Module
- SYS (Mr System System Supervisor)
- System Managers

You can further expand a group to view the list of users:

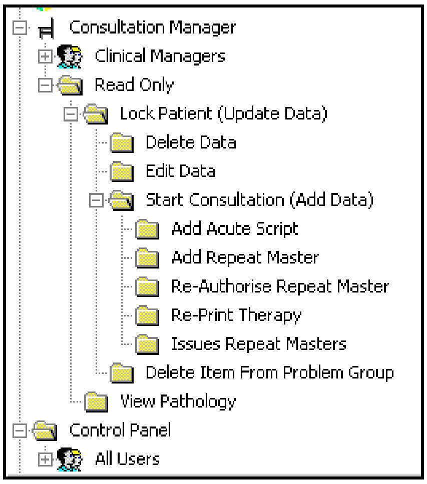


- Security Module
  - SYS (Mr System System Supervisor)
  - System Managers
    - ANNE WHITE - CN (Mrs Anne White)
    - DANIELLE - S&L THER. (Miss Danielle Wilson)
    - DOROTHY - PHYSIO (Mrs Dorothy Mason)
    - DR ALISON HILL (Dr Alison Hill)
    - DR BURTON (Dr David Burton)
    - DR GREEN (Dr Jeff Green)
    - DR MCALLISTER (Dr John Mcallister)

Some modules, such as **Consultation Manager**, **File Maintenance** and **Utilities**, have further menu options once expanded, so there can be different access to the menu options.

In essence, any group that is placed immediately beneath a module heading has access to everything within that module. So if a heading has the group **All Users** immediately beneath, then all users can access that module. Some modules have **Clinical Managers** and others, **System Managers**.

Where the module has further sub-sections, such as **Consultation Manager**, you move from the least secure (Clinical Managers) to a most secure sublevel of **Delete Item**:



- Consultation Manager
  - Clinical Managers
  - Read Only
    - Lock Patient (Update Data)
      - Delete Data
      - Edit Data
      - Start Consultation (Add Data)
        - Add Acute Script
        - Add Repeat Master
        - Re-Authorise Repeat Master
        - Re-Print Therapy
        - Issues Repeat Masters
      - Delete Item From Problem Group
    - View Pathology
- Control Panel
  - All Users

Generally speaking, users or groups are permitted access to the functions they are listed directly under, plus anything which can be followed with a straight line upwards, but not side branches of that straight line.

For example, within the **Consultation Manager Vision Functions**:

Folder	Security Permission
Consultation Manager	If users or groups are added to the Consultation Manager folder, they have full access to **Consultation Manager**.
Read Only	If users or groups are added to the **Read Only** folder, they cannot make any changes, for example, add, edit or delete but can view everything in **Consultation Manager**.
Lock Patient (Update Data)	If users or groups are added to the **Lock Patient** folder, they can view the patient record but not open a consultation or view Pathology results.
Delete data	If users or groups are added to the **Delete Data** folder, they can delete data. If only in this folder, they cannot start a consultation or remove an item from the problem group or view mail for patient.
Edit data	If users or groups are added to the **Edit Data** folder, they can edit data. If only in this folder, they are not able to start a consultation or remove an item from the problem group or view mail for patient.
Start Consultation	If users or groups are added to the **Start Consultation** folder, they can start a consultation and add data. If only in this folder, they cannot edit, delete data, add or print acute and repeat therapy, reauthorize, reprint therapy, do an eReferral, or view mail for patient.
Add Acute Script	If users or groups are added to the **Add Acute Script** folder only, they can start a consultation and add data and add an acute script. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Add Repeat Master	If users or groups are added to the **Add Repeat Master** folder only, they can start a consultation and add data and add a Repeat Master. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Re-Authorise Repeat Master	If users or groups are added to the **Re-Authorise Repeat Master** folder only, they can start a consultation and add data and reauthorise a repeat. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Re-Print Therapy	If users or groups are added to the **Re-Print Therapy** folder only, they can start a consultation and add data and reprint

Folder	Security Permission
	therapy. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Issue Repeat Masters	If users or groups are added to the **Issue Repeat Masters** folder only, they can start a consultation and add data and issue a repeat master. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Choose and Book Referrals	If users or groups are added to the **Choose and Book Referrals** folder only, they can start a consultation and add data and add an eReferral. They cannot edit or delete items unless added to the **Edit** or **Delete** folder.
Delete Item From Problem Group	If users or groups are added to **Delete Item From Problem Group** folder only, they can remove items from problems. If they are only in this folder, they are not able to start a consultation or view mail for patient.
View Pathology	If users or groups are added to **View Pathology** folder only, they can view Pathology and the patient record in Display Only mode.
Add/Edit Patient Warnings	If users or groups are added to **Add/Edit Patient Warnings** folder only, they can add or edit patient warnings.

➔ See **Security Model** on page **32** for full details.

Available Vision Functions and Default Access

Below is a table of **Vision Functions** and the groups that are permitted to access them by default. Some are **All User** access, for example, **Appointments** and others **System Managers** for example, **Control Panel** - **Security**:

Vision module	Functions	Groups permitted access
Appointments	All functions	All Users
	- Restricted Access - - Full Access	
Audit Report	All functions	All Users
Bulk Recalls	All functions	Clinical Managers System Managers
CMS Message Collector	All functions	System Managers
CRPD Data Collection	All functions	Clinical Managers System Managers
	- Start Collection - - Change User ID - - Change audit sequence range	
Clinical Audit	All functions	All Users
	- View Statistics - - View Patients - - Generate Statistics - - - Advanced Generation Options	

Consultation Manager	All functions	Clinical Managers
	- Read Only - - Lock Patient (Update Data) - - - Delete Data - - - Edit Data - - - Start Consultation (Add Data) - - - - Add Acute Script - - - - Add Repeat Master - - - - Re-Authorise Repeat Master - - - - Re-Print Therapy - - - - Issues Repeat Masters - - - - Choose and Book Referrals - - - - Choose and Book Referrals By Proxy - - - Delete Item from Problem Group - - View Pathology - - Add/Edit Patient Warnings - Show Deleted Records	System Managers
Control Panel	All functions	All Users
Daybook	All functions	All Users
	- Create Task - - Complete Task	
Tasks	All functions	All Users
	- Create Task - - Complete Task	
Event Log	All functions	All Users

File Maintenance	All functions	System Managers
	- Maintain Organisations /departments /people - Maintain Staff - Maintain Practice	System Managers System Managers System Managers
GP Communicator	All functions	All Users
GP Summary Bulk Uploads	All functions	Clinical Managers
Global **	All functions	All Users
	- Access to Archived Data - Access to Archived Staff - Access to Archived Patients - RBAC - - Prescribing - - - Print Prescriptions - - - Edit Prescriptions - - - Cancel Prescriptions - - - Sign Prescriptions - - - - Independent Prescribing - - - - Supplementary Prescribing - - - - NPF Prescribing - Configuration - - Patient Record - - - Configure reprint reason - - - Configure repeat inactivation/reactivation reason - - Advance Settings - - - Enable/Disable GP Summary - SCR - - Emergency Access	

	- - Legal Access - - Withdraw	
Items Of Service	No longer applicable	
Mail Administrator	No longer applicable	
Mail Box	All functions	Clinical Managers
Mail Maintenance	All functions	System Managers
Mail Manager	All functions	Clinical Managers
MIQUEST	All functions	System Managers
	- Queries - - Data Collection Agreement Maintenance	All Users
Other Reports	All functions	System Managers
Palliative Care Reports	All functions	All Users
Patient Groups	All functions	Clinical Managers System Managers
Pocket Vision	All functions	Clinical Managers
Queued GP Summaries	All functions	Clinical Managers
Registration	All functions	All Users
	- Read Only - - Update Patient records - - - Change Spine Sharing Consent - - - Add Sensitive Records	

	- - Security Controlled Transactions - - Merge Patients - - Transfer Patients	System Managers
Registration Links	All functions	System Managers
	- Standard Actions - - Security Controlled Actions	All Users
SCR Viewer	All functions	Clinical Managers
Search & Reports	All functions Also allows access to the Vision+ Practice Reports module.	All Users
Security module	All functions	System Managers
THIN Data Collection	All functions	Clinical Managers System Managers
	- Start Collection - - Change user ID - - Change audit sequence change	All Users
Vision Utilities	All functions	
	Populate Problems Drug Dictionary Utilities Populate Read formulary *BRU Weekly Report OXMIS - Read retrofit utility Populate CMS Suitability Priority Update	All Users Clinical Managers System Managers Clinical Managers System Managers Clinical Managers

		Clinical Managers Clinical Managers System Managers

See **Vision Functions** on page **19** and **Security Model** on page **32** for further details.

* **BRU** - A weekly report generated to the Birmingham Research Unit.

** **Global** includes access to archived data, archived staff and archived patients:

- **Archived data** on **Consultation Manager** is the data viewed when you select **Options** - **Show Deleted Records**.
- **Archived Patients** are those that can be viewed when you click off the **Active Patients Only** tab on the **Select Patient** screen.
- **Archived Staff** are those staff that are made inactive on the **Staff** - **Personal** screen in **File Maintenance**.

See **Minimum Permissions for Using Web Services** on page **28** for details.

Minimum Permissions for Using Web Services

Web Services is part of the mechanism that enables **Vision 3** and **Vision Anywhere** to communicate. The following is a list of the minimum security settings required for Web Services to work. It is essential that any of your staff that are to use **Vision Anywhere** have the following permissions:

- **Appointment - Restricted Access**
- **Consultation Manager - Delete Data**
- **Consultation Manager - Add Acute Script**
- **Consultation Manager - Add Repeat Master**
- **Consultation Manager - Re-Authorise Repeat Master**
- **Consultation Manager - Re-Print Therapy**
- **Consultation Manager - Issues Repeat Master**

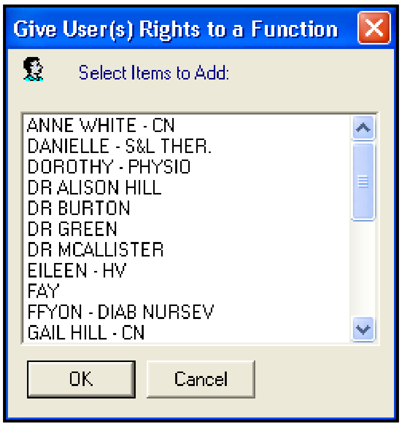
Adding and Removing Users and Groups from Vision Functions

From **Management Tools** - **Control Panel** - **Security**, the quickest way to add a user or group to a **Vision Function** is to click, drag and drop a staff member or group from the left pane on to the required **Vision Function** on the right.

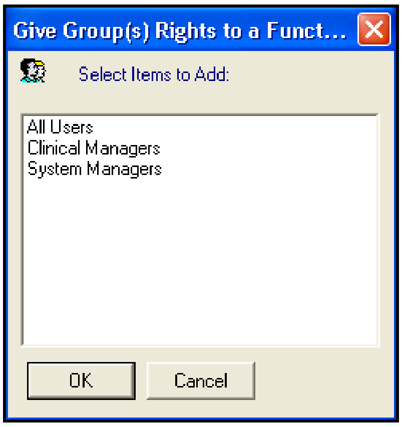
Alternatively, from the **Vision Function** pane, right click the function required and select either:

- **Add User(s) to Function** - To select individual user(s) to be added to a function.
- **Add Group(s) to Function** - To select a group to be added to a function:

Training Tip - You can select more than one user or group at a time by holding down **Ctrl** on your keyboard and selecting on the items you require, or a block of users or groups by selecting the top one in the list required, holding the **Shift** key on your keyboard and selecting the bottom one in the list required.



ANNE WHITE - CN
DANIELLE - S&L THER.
DOROTHY - PHYSIO
DR ALISON HILL
DR BURTON
DR GREEN
DR MCALLISTER
EILEEN - HV
FAY
FFYON - DIAB NURSEV
GAIL HILL - CN



All Users
Clinical Managers
System Managers

To remove a user or group from a **Vision Function**, highlight the user or group, right click and select either:

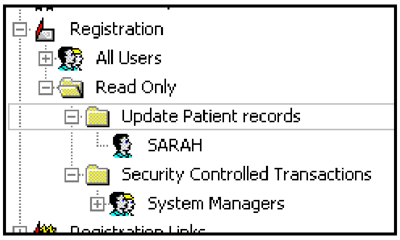
- **Remove User from Funct**ion, or
- **Remove Group from Function**.

If, for example, you want to allow access to **Registration** for some staff, so they can register permanent and temporary patients, but you do not want these staff to access the **Security transactions**, as this allows them to deduct patients.

1. From the **Vision 3** front screen, select **Management Tools** - **Control Panel** - **Security**.
2. Create two groups:
    - A group of users who can access everything in **Registration**, and
    - A group who can update records but cannot access **Security transactions** in **Registration**.

See **Adding a New Security Group** on page **16** for details.

3. On the right-hand side under **Vision Functions**, select and expand the **Registration** section. By default, the group **All Users** is immediately below, unless you have previously altered this.
4. Right click on **All Users** and select **Remove Group from Function**.
5. Right click on **All Users** again and add in the group who are allowed to do everything.
6. Select **Expand** ⊞ next to **Registration - Read Only**, to expand that section and then right click on **Update Patient Records** and select **Add User to Function**, or **Add Group to Function**, and select your restricted user or group:



```
Registration
  All Users
  Read Only
    Update Patient records
      SARAH
    Security Controlled Transactions
      System Managers
```

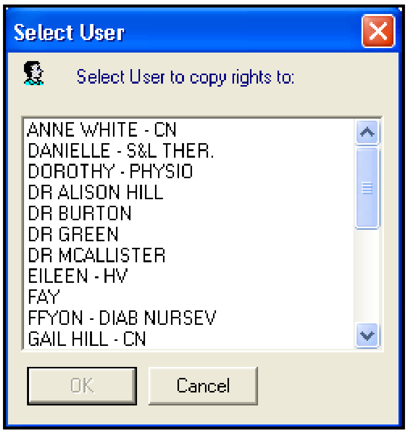
7. Select **OK** to save.

For the users in the restricted group, **Security (Transactions)** no longer displays in **Registration**, but they can still update and add patient details.

Copy Rights to Another User

If you have determined the security rights of a user, and want another user to share similar rights, you can copy these over.

1. From **Management Tools** - **Control Panel** - **Security**, in the **Current Users**, highlight the staff member whose rights you have already determined.
2. Right click on them and select **Copy rights to another user**.
3. The **Select User** screen displays, select the new user to whom you want these rights copied and select **OK**:



Select User

Select User to copy rights to:

ANNE WHITE - CN
DANIELLE - S&L THER.
DOROTHY - PHYSIO
DR ALISON HILL
DR BURTON
DR GREEN
DR MCALLISTER
EILEEN - HV
FAY
FFYON - DIAB NURSEV
GAIL HILL - CN

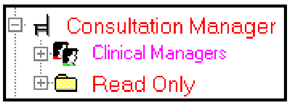
Security Model

Vision 3 security uses a hierarchical model to represent the individual modules. Think of this model as a tree (albeit, upside-down). The root of the tree is the module itself, for example, **Consultation Manager**. When we expand the root, we see other functions within the module. If these functions can also be expanded, they are called branches, if they cannot, we call them leaves.

Groups and users added at the root have access to all parts of the tree. This is for convenience, so you do not have to define what parts of a module a group can or cannot access.

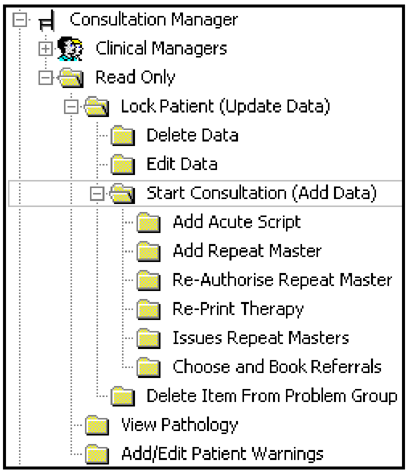
Groups added to branches or leaves have access granted by their position in the tree. The first level of branches from the root is the least secure, and the leaves are the highest.

For example, if you expand **Consultation Manager**, a group of **Clinical Managers** displays, they can access all functions within **Consultation Manager**. There is a further option of **Read Only**, this is the lowest category of security, someone who can look at **Consultation Manager** but not make any entries:



- Consultation Manager
  - Clinical Managers
  - Read Only

Once again, you can select **Expand** ⊞ to expand the list further:

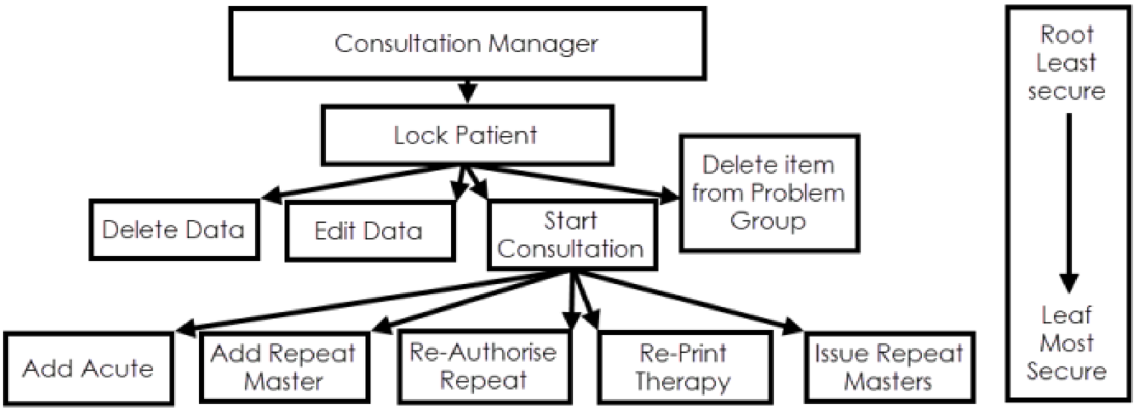


- Consultation Manager
  - Clinical Managers
  - Read Only
    - Lock Patient (Update Data)
      - Delete Data
      - Edit Data
      - Start Consultation (Add Data)
        - Add Acute Script
        - Add Repeat Master
        - Re-Authorise Repeat Master
        - Re-Print Therapy
        - Issues Repeat Masters
        - Choose and Book Referrals
      - Delete Item From Problem Group
    - View Pathology
    - Add/Edit Patient Warnings

The default is illustrated above for **Consultation Manager**, where the **Clinical Managers** group is in the immediate level beneath the **Consultation Manager** heading giving all **Clinical Managers** all rights.

Visualise the tree being upside-down, the root being **Consultation Manager**.

The users or groups here have access to all of **Consultation Manager**, the root represents the least secure access. The leaves are the most secure access to the module:



A path traversing the tree from the root to a leaf moves through increasing access restriction, from the least secure at the first branch to the most secure at the leaf. Paths in the tree are set so that rights follow system logic.

For example, to delete data we must first lock the relevant patient record, so **Delete Data** is a leaf of the **Lock Patient**.

Users added at the root are given access to everything within the tree. This all rights permission granted at the node are checked first. If a user or group is found here, then they are assumed to have all rights and checking stops.

If a user is not found at the root, checking begins at the first level of the tree. Groups or users found here are assumed to have incremental rights.

Incremental rights grant permissions to all leaves between the branch to which the group or user is added and the root, but a group or user is refused access to anything in its sub-tree. The permissions of a group or user are determined by the path that is traced between it and the root. Permissions only apply to the path from the leaf to the root; they do not include any other leaves on that level.

For example, a group or user added at the **Lock Patient** leaf would have access to **Lock Patient** and **Consultation Manager**, but not to other leaves.

A group or user added to **Start Consultation** would have access to **Start Consultation**, **Lock Patient**, and **Consultation Manager**, but not to **Delete Data**, **Edit Data**, **Delete from Problem Group**, which are on the same level but not on the branch.

See **Vision Functions** on page **19** for more details.