
Security

User Guide – V 12.0

June 10, 2024



Parklane Systems - All Rights Reserved

No part of this publication may be reproduced, transmitted, transcribed, or translated into any language in any form or by any means; electronic, mechanical, manual or otherwise, without prior written permission from Parklane Systems Inc., London, Ontario.

This document is strictly proprietary to, and for the sole use of, the person(s) as determined by Parklane Systems Ltd. It is against the law to transfer this document or any associated document for any purpose without prior written permission of Parklane Systems Ltd.

While reasonable efforts have been taken in the preparation of this guide to assure its accuracy, Parklane Systems Ltd. assumes no liability from any errors or omissions from the use of the information contained herein.

Parklane Systems Security

Introduction

Use Security to indicate each user account system access rights regarding:

- Modules; and in each module:
 - Menu Items
 - Data/screens access
 - Functions that can be used
 - Various rules
- Department restrictions
- Company restrictions (multi-company option only)

For each user account, you will provide:

- Name
 - 25 characters
- Id
 - 10 characters
 - Identify the account using a name abbreviation.
 - Used by the system for identification and auditing purposes
- Password
 - 10 characters
 - Passwords are hashed
 - Criteria for valid passwords can be established under “Sign-In Rules” located on the Main Menu
- Email Address

There are four types of Security records:

- Role profiles where access rights can be identified for a group of user accounts.
- Role based accounts that use the rights identified in particular role.
- Unique user accounts that are not affiliated with a role and the rights are specific to that user.
- Restricted Administrators (Multi-company option only) where a user is given access to Security to manage their own user accounts within one company.

How it Works

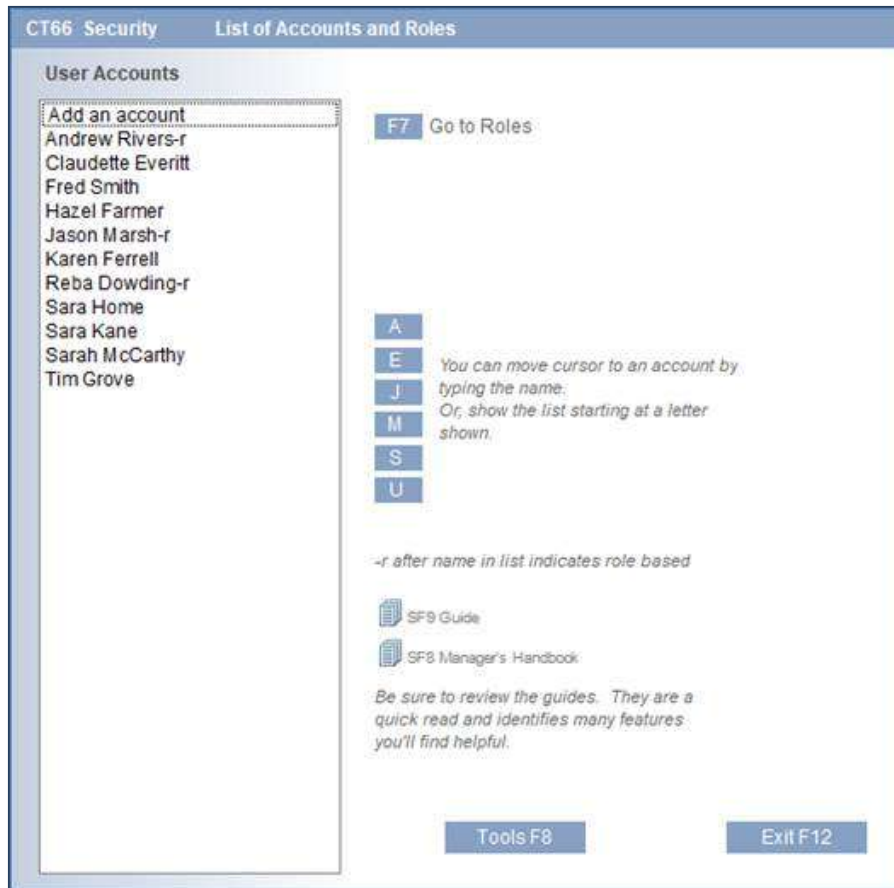
It is important that Managers have access to Security. There are many useful tools and controls that can be used by a Manager, however, one would need to use and appreciate Security to determine what fits their needs.

Parklane Support provides instructions to access Security for the first time.

The first record will be a unique user account that is defined as an Administrator with access to Security. Once this account has been set up, Security is available to that person on the Main Menu.

Below is the Security home screen.

- To add a unique user account, select “Add an Account”
- To access a current account, select the account from the list.
- To manage your role profiles, select F7 Go to Roles.
- To add a Restricted Administrator, select “Add an account”.



Note that accounts listed with “-r” after their name were added under a role and use the rights as defined in that role.

Adding a Unique User Account

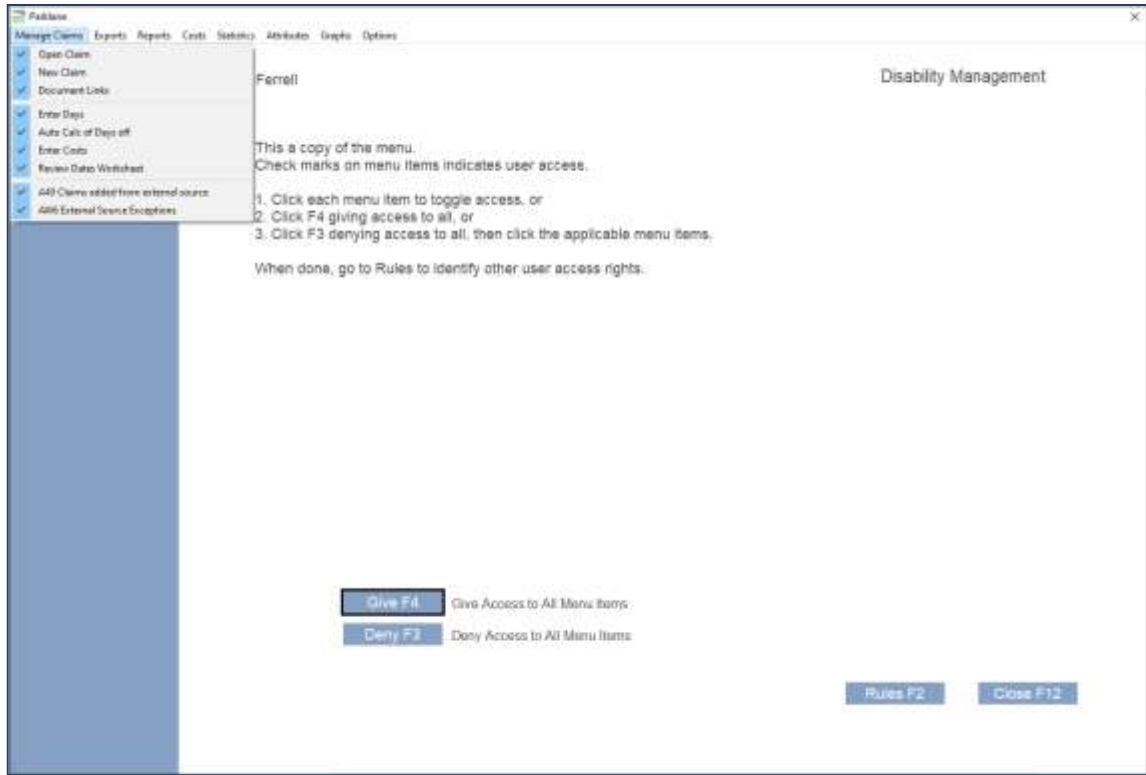
After selecting “Add an Account”, on the next screen (below) complete:

1. Name, User Id, Password, Email Address
2. Select the modules that may be accessed
3. If the user is restricted to specific departments, check “Has department restrictions”.
A button will appear to allow you to define which departments.
4. Select F1 at the bottom of the screen to indicate the menu, data & rules rights in each module.

Select a module from the list to proceed to its menu.

From the menu check the applicable menu items or, select F4 to give access to all menu items.

Then select F2 to identify the Rules.



Below is a sample of the Rules. They vary by module.

The left lists the input screens available in the module. Give access to all or chose specific screens.

The right lists actions that may or may not be allowed. The example below indicates that the user may not cancel a record or change comments entered by another user.

Initially, it is recommended that Nutshell not be used until the users are familiar with the system.

Disability Management - Data Access & Rules

Karen Ferrell

Check the screens this user has access to

- ☐ Check all
- ☒ Record Description
- ☒ Medical Condition
- ☒ Medical Part 2
- ☒ Benefits & Reporting
- ☒ Attributes
- ☒ General Comments
- ☒ Confidential Comments
- ☒ Days & Costs Summary
- ☒ Review Dates
- ☒ Appointments
- ☒ Form Letters
- ☒ Key Notes
- ☒ Document Folder
- ☒ Document Links
- ☒ Guideline Worksheet
- ☒ Report A72 Claim Details
- ☒ TMS Audit
- ☒ User Notes & Email
- ☒ Demographics
- ☒ Time Markers

Check the rules that apply to this user:

- ☐ Check all
- ☒ Allow: Access to claims from reports
- ☒ Allow: See cancelled claims in claims list
- ☒ Allow: Ability to cancel a record
- ☒ Allow: Changes to Reference Number
- ☒ Allow: Changes to Guideline Website URLs
- ☐ Reason: Mandatory. Must be completed
- ☐ Allow: Deleting Document Links
- ☐ Disallow: Adding Document Links
- ☐ Add Doc. Links only. Trumps rules above
- ☒ Allow: Changes to Document Folders
- ☒ Allow: Changes to General Comments
- ☐ Add Comments only. Trumps rule above
- ☒ Allow: Changes to Confidential Comments
- ☐ Add Confid. Comments only. Trumps rule above

Nutshell F2 If you gave access to in-a-Nutshell, complete the Nutshell Profile using the F2 button. Once you have completed this profile, the same rules will apply to all modules.

Close F12

Adding a Role Profile and the Role-based Accounts

Enter the Role Profile by using the same procedure for a Unique User Account.

Once established, you can identify accounts that would use this role profile.

Role Profiles may be copied and then modified for ease of setup.

C120: Role

F8 List of Roles F9 Add new Role SF7 Delete Record

Role Name:

1) Modules that may be accessed

<input type="checkbox"/> Security & Login Rules	<input type="checkbox"/> Work Accommodation	<input type="checkbox"/> Maintenance
<input type="checkbox"/> Personal Data	<input type="checkbox"/> Attendance	<input type="checkbox"/> Audiometric
<input type="checkbox"/> Incident Reporting	<input type="checkbox"/> Simon	<input type="checkbox"/> Patient
<input type="checkbox"/> Recall	<input type="checkbox"/> Risk Hazards	<input type="checkbox"/> Event
<input type="checkbox"/> Disability Management	<input type="checkbox"/> Risk Tasks	<input type="checkbox"/> Task Manager
<input type="checkbox"/> Chart <input type="checkbox"/> Lifestyle	<input type="checkbox"/> Incident Investigation	<input type="checkbox"/> Diary
	<input type="checkbox"/> Daily Activity Stats	

2) Restrictions or access rights

☐ ***Has company restrictions

☐ ***Has department restrictions

☐ Hide SIN/SSN from user (excludes Government forms)

☐ May Sync SQL Database

☐ **May run process to purge/destroy old data records

☐ May access the Privacy Audits & Logs located on the Main Menu

3) Module Restrictions

F1

After checking the modules this user/role may access, indicate their access rights in each module.
Which menu items can be used.
What information can be accessed.
What actions are allowed.

**See under Options in Personal Data

***Check restrictions only if the restrictions will apply to all accounts.
You may optionally identify restrictions that are unique to each account under this role.

Exit F12

Company and Department Restrictions

(Company Restrictions apply to those who use Parklane's multi-company option)

You have three options here:

- If all accounts will be restricted to the same companies/departments, you may identify those restrictions on this screen.
- If the restrictions vary by account, leave these boxes unchecked. You may then identify at the account level.
- You may restrict certain companies/departments that will apply to all accounts; then identify additional restrictions for certain accounts.

Once you have completed the above screen, Select F2-Manage Accounts to manage the accounts under this role profile.

Managing Accounts for Role Profiles

Role Profiles – Managing Accounts

CT2X Role

Role Name: **Security Team**

1) Access that may be accessed:

- ☐ Security & Login Rules
- ☐ Personal Data
- ☐ Incident Reporting
- ☐ Recall
- ☐ Disability Management
- ☐ Check Lifestyle
- ☐ Risk Accommodation
- ☐ Attendance
- ☐ Search
- ☐ Risk History
- ☐ Incident Investigation
- ☐ Daily Activity Data
- ☐ Maintenance
- ☐ Audiotextic
- ☐ Patient
- ☐ Test Manager
- ☐ Query

2) Restrictions of access rights:

- ☐ Has company restrictions
- ☐ Has department restrictions
- ☐ Hide SSOSS from user (excludes Government forms)
- ☐ May Sync SSO Credentials
- ☐ May not proceed to purge/delete old data records
- ☐ May access the Privacy Audit & Log located on the Main Menu

3) Access Restrictions:

F1

Any checking the restriction by controls may access, indicate that access rights in each module. When many items can be added. What information can be accessed. What actions are allowed.

4) Check restrictions only if the restrictions will apply to all accounts. You may optionally check restrictions that you want to search against under this box.

Manage Accounts: F2

Save Role Profile: F1

Save F10

Select F1 to add a new account.

CT2X Accounts

Role: **Attendance Support**

**Jimmy Twoshoes
santa claus**

Add new account

F1

Enter Name, User Id, Password, Email Address and applicable restrictions.

CT2Y User Account

Name:

User Id:

Password: **SF8** Reset

Password Date:

Last Signin Date:

Email Address:

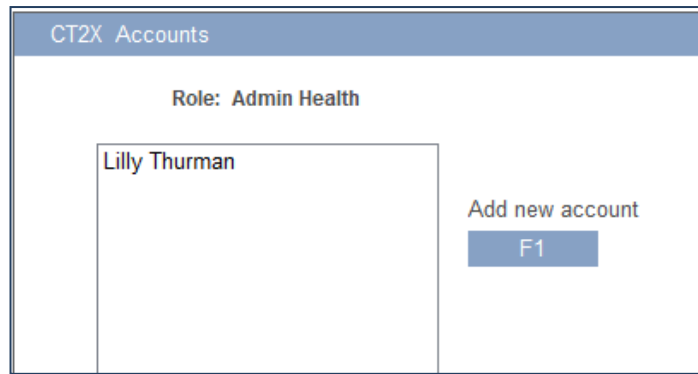
☐ Has company restrictions **F4** Select Companies

☒ Has department restrictions **F3** Select Departments

Close F12

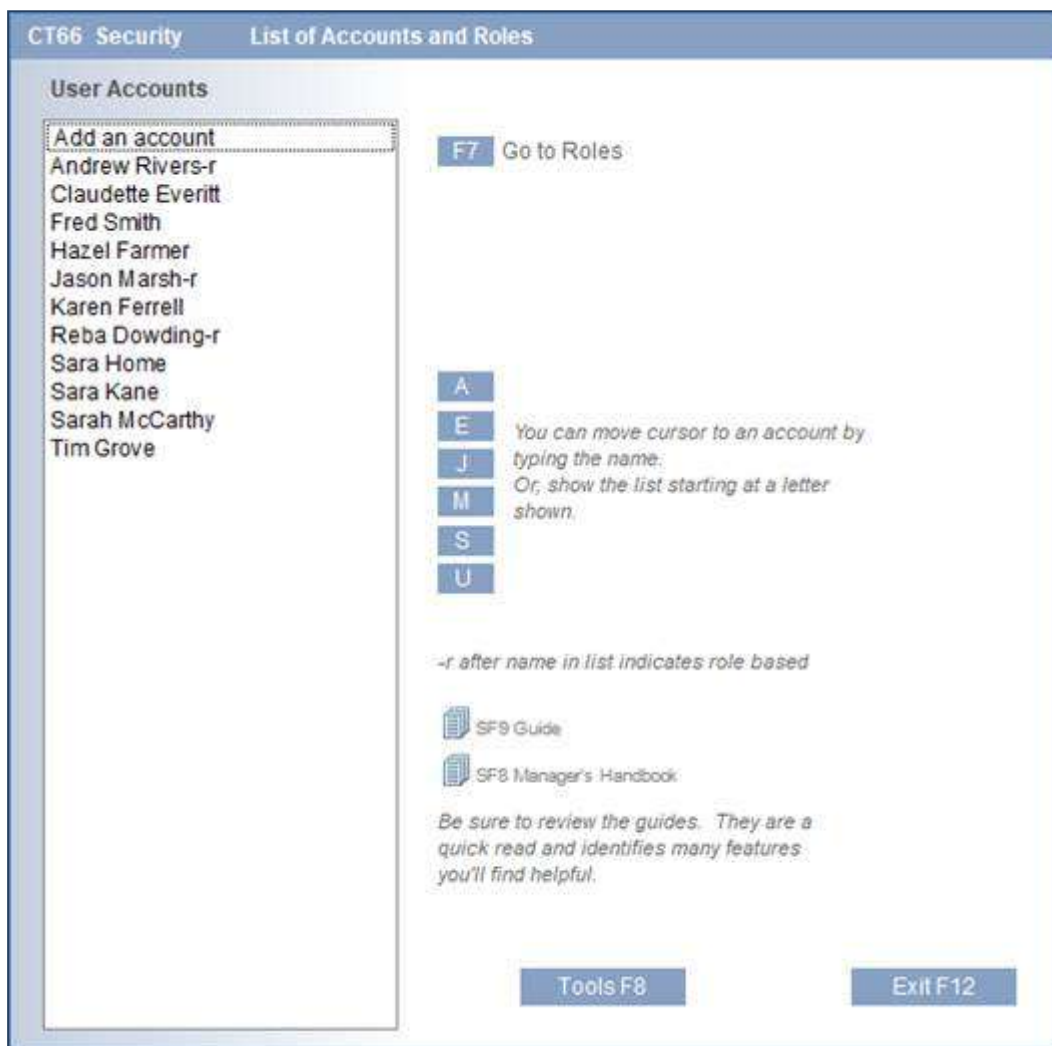
SF7 Delete Record

Repeat to add additional accounts.



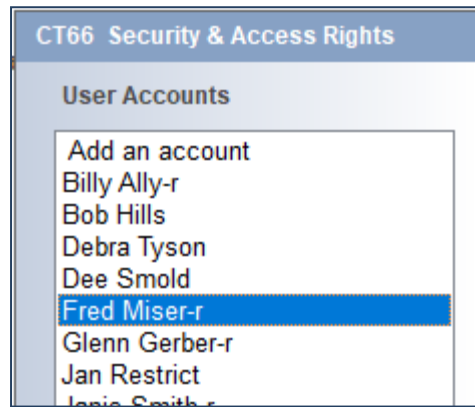
Notes re: Role Profiles

1. The Role Profile can be modified after accounts are added.
2. The accounts will appear on the Home screen in the list of accounts.
"-r" at the end of each name indicates the account is Role based.



Assigning an Account to another Role

Select the account.



Select F6-Change Role.

The screenshot shows a window titled 'CT20 User Account'. At the top, it says 'Using Role: Clerk - General'. There are buttons for 'Exit List of accounts', 'F3 Add account', and 'SF7 Delete Record'. The account details for 'Jason Marsh' are shown, including 'Account Id: MARSH', 'Password', 'Password Date: 15/09/2023', and 'Password hashed & secured'. A button 'F6 Change Role' is highlighted. Below this, there are three sections: '1) Modules that may be accessed', '2) Restrictions or access rights', and '3) Module Restrictions'. The 'F1' button is also highlighted in section 3.

1) Modules that may be accessed

- ☐ Security & Login Rules
- ☒ Personal Data
- ☒ Incident Reporting
- ☐ Recall
- ☐ Disability Management
- ☐ Chart
- ☐ Lifestyle
- ☐ Work Accommodation
- ☐ Attendance
- ☐ Simon
- ☐ Risk Hazards
- ☐ Risk Tasks
- ☐ Incident Investigation
- ☐ Central Access
- ☐ Daily Activity Stats
- ☐ Maintenance
- ☐ Audiometric
- ☐ N.E.E.R.
- ☐ Patient
- ☐ Event
- ☐ Task Manager
- ☐ Diary
- ☐ Customer Care

2) Restrictions or access rights

- ☐ Has department restrictions
- ☐ Hide SIN/SSN from user (excludes Government forms)
- ☐ May hide some employees from other users
- ☐ May run Consolidation
- ☐ **May run process to purge/destroy old data records
- ☐ May access the Privacy Audits located on the Main Menu
- ☐ Is a Security Admin who is restricted to one company in Security

3) Module Restrictions

After checking the modules this user/role may access, indicate their access rights in each module.

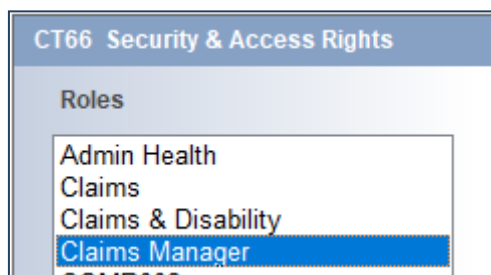
- Which menu items can be used.
- What information can be accessed.
- What actions are allowed.

F1

F6 Ontario E-Form? Passwords

Exit F12

Select the new Role



Any company/department rights that were previously specific to that account remains.

CT20 User Account

Using Role: Claims Manager

Account Name: Fred Miser

Account Id: C2

Password: [SF8] Reset

Email Address: []

Password Date: 19/04/2021

Last Sign in Date: 19/04/2021

Password hashed & secured

Adding a Restricted Administrator (Multi-company option only)

Under the multi-company option, you may set-up administrators who will manage accounts under their assigned company only.

1. Add a user account.
2. Check:
 - a. Security & Login Rules
 - b. Is a Security Admin who is restricted to one company in Security
 - c. The modules the administrator has access to
(Note that the administrator can also modify the module access rights)
 - d. Has Company Restrictions & select the one company
 - e. F1 Module Restrictions

The screenshot displays the 'CT20 User Account' form. At the top, there are buttons for 'Go List of accounts', 'F9 Add account', and 'SF7 Delete Record'. The form fields include:

- Account Name: Sara Kane
- Email Address: s.kane@parklanesys.com
- Account Id: SARA
- Password: (with a 'SF8 Reset' button)
- Password Date: (with a 'Password hashed & secured' status)
- Last Sign in Date: 29/11/2023

Below the form fields, there are three main sections for configuring user access:

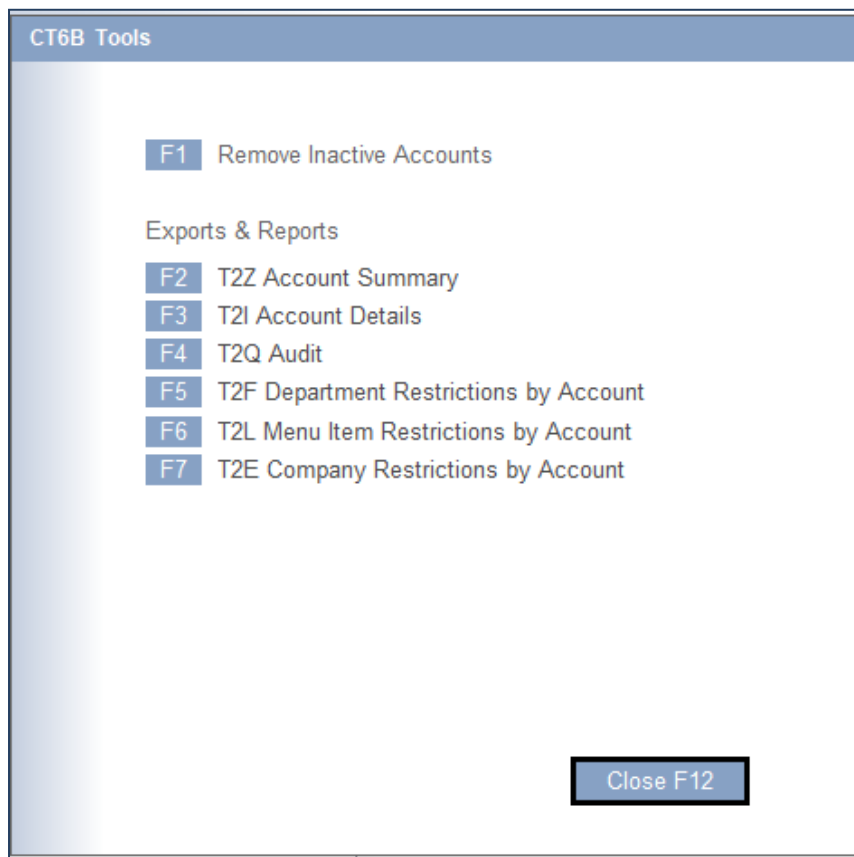
- 1) Modules that may be accessed:**
 - ☒ Security & Login Rules
 - ☒ Personal Data
 - ☒ Incident Reporting
 - ☒ Recall
 - ☒ Recall Restrictions (SF2)
 - ☒ Disability Management
 - ☒ Chart
 - ☐ Lifestyle
 - ☒ Work Accommodation
 - ☒ Attendance
 - ☒ Simon
 - ☒ Risk Hazards
 - ☒ Risk Tasks
 - ☒ Incident Investigation
 - ☒ Central Access
 - ☒ Daily Activity Stats
 - ☒ Maintenance
 - ☒ Audiometric
 - ☐ N.E.E.R.
 - ☐ Patient
 - ☒ Event
 - ☐ Task Manager
 - ☐ Diary
 - ☐ Customer Care
- 2) Restrictions or access rights:**
 - ☒ Has company restrictions (F4 Select Companies)
 - ☐ Has department restrictions
 - ☐ Hide SIN/SSN from user (excludes Government forms)
 - ☒ May hide some employees from other users (SF3 Info)
 - ☐ **May run process to purge/destroy old data records
 - ☐ May access the Privacy Audits located on the Main Menu
 - ☒ Is a Security Admin who is restricted to one company in Security
 - ☒ Ontario E-Form? Passwords (SF6)
- 3) Module Restrictions:**
 - ☒ F1

After checking the modules this user/role may access, indicate their access rights in each module:
 Which menu items can be used.
 What information can be accessed.
 What actions are allowed.

At the bottom right, there is an 'Exit F12' button. A note at the bottom center states: '**See under Options in Personal Data'.

Security Tools

There are some tools that will help you manage your user accounts more effectively. On the Home screen, select F8 Tools.



F1 Remove Inactive Accounts

- Helps you easily establish retired accounts that should be removed.

CT6A Remove Inactive User Accounts

Last Login	Name
<input type="checkbox"/> No date	Billy Ally
<input type="checkbox"/> No date	Bob Hills
<input type="checkbox"/> No date	Glenn Gerber
<input type="checkbox"/> No date	Jan Restrict
<input type="checkbox"/> No date	Janis Smith
<input type="checkbox"/> No date	John Smith
<input type="checkbox"/> No date	Lisa Smith
<input type="checkbox"/> No date	Victoria Lansing
<input type="checkbox"/> 14 Apr 21	Dee Smold
<input type="checkbox"/> 15 Apr 21	Linda Bills
<input type="checkbox"/> 19 Apr 21	Fred Miser
<input type="checkbox"/> 21 Apr 21	Debra Tyson

This list is sequenced by last sign-in date. A missing date indicates the account has never been used or not since Q2, 2021.

Check the accounts you want removed. Select F5 to remove the accounts that have been checked.

Accounts removed will be recorded in the Audit.

On completion, Security will close and return to the Main Menu,

Remove F5

Close F12

F2 Account Summary

- Provides a quick glance of the accounts and can be used to ensure that each account has the necessary criteria such as email address.

A	B	C	D	E	F	G	H	I
Account	Name	Uses Role	Role Used	Email	Last Sign in	Restr Admin	Dept Restr	Comp Restr
GLENNGE	Glenn Gerber	Y	Claims Manager		13/03/2021			
JANRE	Jan Restrict				01/04/2021	Yes		Yes
BOBHI	Bob Hills				02/04/2021			
LISASM	Lisa Smith	Y	Claims Manager	L.Smith@myco.com	10/04/2021			
JOHNS	John Smith				01/03/2021			
VLANSING	Victoria Lansing			V.Lansing@myco.com	09/04/2021			

F3 Account Details

- Shows list of all role profiles and user accounts
- Lists all modules each account has access to (for both unique accounts and those that use a role)

A	B	C	D	E	F	G	H	I	J	K
Account	Name	Uses Role	Role Used	Security	Personal	Incidents	Recall	Disability	Chart	Work Acc
.Role Profile	Claims Manager		Claims Manager		Y			Y		Y
.Role Profile	Occupational Health		Occupational Health		Y	Y		Y		Y
GLENNGE	Glenn Gerber	Y	Claims Manager		Y			Y		Y
JANRE	Jan Restrict			Y	Y		Y	Y	Y	Y
LISASM	Lisa Smith	Y	Claims Manager		Y			Y		Y

F4 Audit

- System tracks all actions and maintains an audit of resulting changes

A	B	C	D	E	F	G	H	I	J	K	L
Date	Time	Account Id	Name	Administrat	Admin Na	Action	Role Profile	Uses Role	Role Used	Security	Personal
01/04/2021	8:41	GLENNGE	Glenn Gerber	SusanL	Susan Lan	Add					Y
01/04/2021	8:41	GLENNGE	Glenn Gerber	SusanL	Susan Lan	Access					
01/04/2021	8:42	GLENNGE	Glenn Gerber	SusanL	Susan Lan	Access					
01/04/2021	8:42	LARRYB	Larry Billis	SusanL	Susan Lan	Delete		Y			

F5 Department Restrictions by Account

A	B	C	D	E
ID	Name	Company	Dept Code	Department
BOB	Bob Hills	All		
LINDAB	Linda Bills	1	FINANCE	Finance
LINDAB	Linda Bills	1	HEALTH	Employee Health
LINDAB	Linda Bills	1	HR	Human Resources
LINDAB	Linda Bills	1	IT	Information Technology

F6 Menu Item Restrictions By Account

- By module, shows menu items that can be accessed by each account

A	B	C	D	E	F
ID	Name	Module	Menu Item	Access Yes	Access No
FREDM	Fred Miser	DisMngr	Open Claim	Yes	
FREDM	Fred Miser	DisMngr	New Claim	Yes	
FREDM	Fred Miser	DisMngr	Document Links	Yes	
FREDM	Fred Miser	DisMngr	Enter Days	Yes	

F7 Company Restrictions by Account

- For those with Multi-company option only

CT99 View Report					
F8] Search <input type="text"/>		F5 Print	SF5 Print to Pdf	Page Up Page Down	Home End
Parklane Systems London Ontario, Drive D				Page	0001 T2E
Security				Date	21 Apr 21
Company Access				Time	12:21
User ID	User Name	Company Access			
BOB	Bob Hills	All			
C2	Fred Miser	All			
DD	Billy Ally	All			
DE	Linda Bills	All			
DEB	Debra Tyson	All			
GLENNGE	Glenn Gerber	All			
JOHNS	John Smith	All			
LISASM	Lisa Smith	All			
VLANSING	Victoria Lansing	All			

Parklane Systems Inc.
10-521 Nottinghill Road
London, ON N6K 4L4
Canada
519.657.3386
ContactUs@parklanesys.com

Access the Parklane web site for more details about Parklane products

www.parklanesys.com