DOMINO

Domino D-Series
Pharma User Guide

D120i

D320i

D620i

THIS PAGE INTENTIONALLY LEFT BLANK

CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

INTRODUCTION

This Pharma User Guide covers the D-Series Laser Marking System operated via the remote TouchPanel, or via a PC with Quickstep software installed and running Microsoft Windows 7® or Microsoft Windows 8®.

It describes the functionality specific to the Pharma version of the D-Series Laser Marking System. This includes the user-id and password system, and the electronic signatures and electronic records functionality.

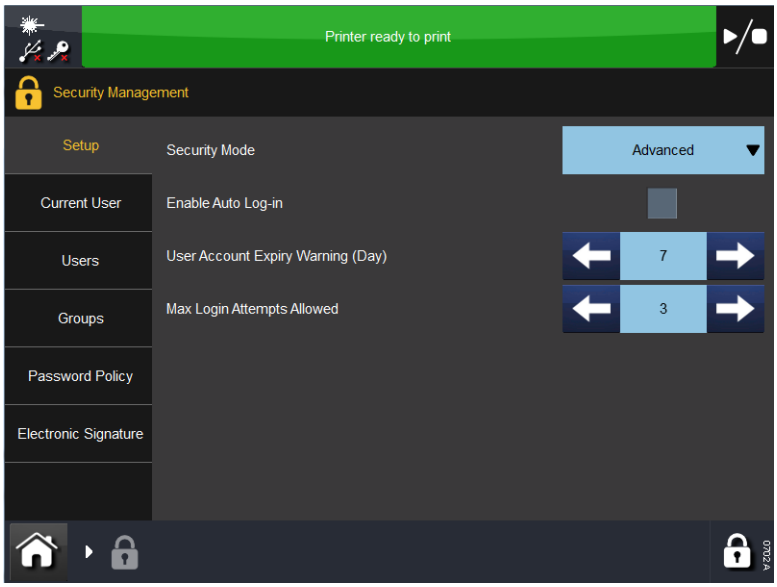
Note: *A Domino Pharma Key must be fitted to the controller and the Security Mode set to 'Advanced' in order to enable the user-id and password, and the electronic signature and records functionality.*

Please refer to the D-Series Product Manual for details of non-pharma functionality.

SETUP

(1) Login using the Administrator Username and Password.

(2) Select *Settings* > *Security* > *Setup*.



(3) If not selected, click on the *Security Mode* drop-down arrow and select *Advanced*.

Enable Auto Log-in: Only select this if you wish to allow automatic log-in for a selected user

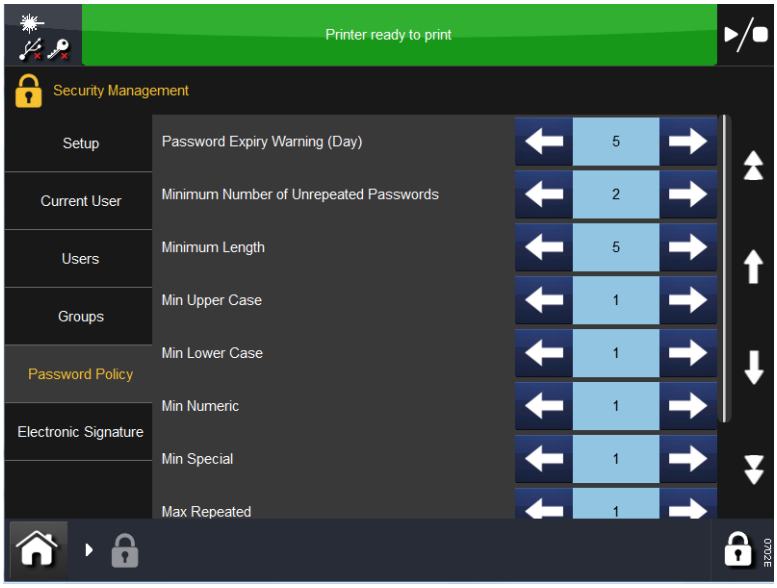
Auto Login User: Select the user from the drop-down list.

User Account Warning (Days): Enter how many days before a user's account is due to expire, an on-screen reminder should be displayed.

Max Login Attempts Allowed: Enter maximum number of unsuccessful logins permitted before an account is locked.

PASSWORD POLICY

Select *Settings* > *Security* > *Password Policy.*



The following can be set:

- Password Expiry Warning (Days).
- Minimum Number of Unrepeated Passwords - number of new passwords used before repeating a password.
- Minimum Length.
- Min Upper Case.
- Min Lower Case.
- Min Numeric.
- Min Special - selected special characters.
- Max Repeated - maximum number of duplicated characters a password may contain.
- Max ID Characters - maximum number of character matches with the user-id a password may contain.
- Special Characters - enter the required special characters (any keyboard character can be selected).

GROUPS

A group consists of a selected number of user permissions. The D-Series is delivered with four default groups: Administrator, Logout, Operator and Supervisor, each with their own set of selected permissions. However, each group's set of permissions can be changed, if required.

New and existing users inherit permissions by being associated with one or more Groups.

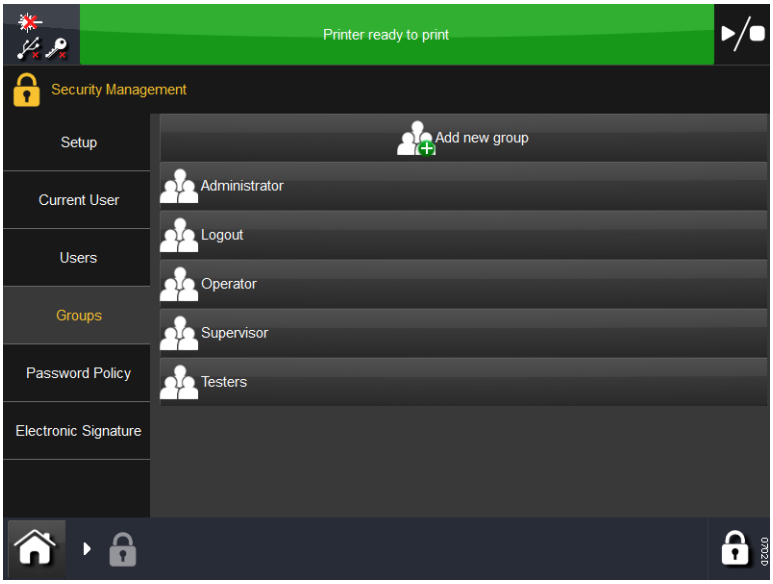
New Groups, with required permissions, can also be added.

ADDING NEW GROUPS

This feature allows Groups with selected permissions to be created. Users associated with one or more of these groups will then inherit the permissions of the group(s).

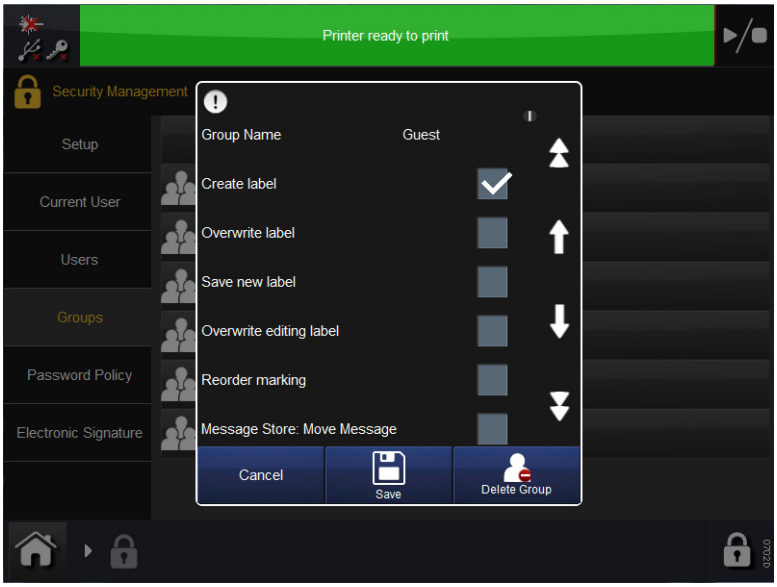
(1) Select *Settings* > *Security* > *Groups*.

(2) Select *Add new group*.



(3) Enter a new 'Group Name' and select *Save*.

(4) Select the check box of each of the permissions required for the Group.



(5) Select *Save* to display the new group in the list of Groups.

DELETING GROUPS

(1) Select *Settings* > *Security* > *Groups*.

(2) Select the required Group from the Groups list and select *Delete Group*.

(3) Select *OK* to confirm the deletion.

CHANGING PERMISSIONS

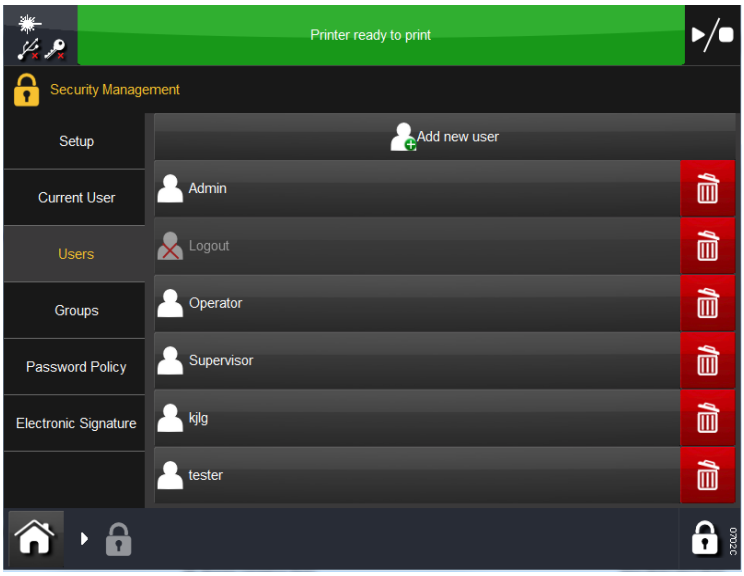
(1) Select *Settings* > *Security* > *Groups*.

(2) Select the required Group and change the permissions, as required.

(3) Select *Save* to confirm the changes.

ADDING NEW USERS

(1) Select *Settings* > *Security* > *Users.*



(2) Select *Add new user.*

User Name: enter the required User Name (i.e. user-id.).

Password: enter chosen password.

Retype Password: i.e. confirm the password.

Groups: From the drop-down list, select the Group or Groups whose permissions are required for the new user.

Status: From the drop-down list, select *Active, Dormant* or *Locked*.

Ensure that the *Must change password* check box is selected to force the new user to change their password when they login for the first time.

If required, enter the new user's *Forename, Surname* and *Department*.

Inactivity Timeout in Minutes: If required, set the period of user inactivity that will prompt an automatic logout.

Account Expiry Enabled: Select the check box to enable.

Account Expiry Date: If required, select the date on which the user's account will automatically expire.

Password Expiry Days: the number of days after which the user's password will expire and a new password will need to be created.

DELETING USERS

Note: The Delete action cannot be undone.

(1) Select *Settings* > *Security* > *Users.*

(2) Select the relevant user's Delete symbol  .

(3) Select *OK* to delete the user.

CHANGING USER PASSWORDS

(1) Select *Settings* > *Security* > *Users* and select the required user.

(2) Select and then enter and verify (retype) the new password.

(3) Select *Change* and then *Save* to change the password.

CHANGING USER STATUS

The user status can be changed from the current status (e.g. "Locked") to a new status (e.g. "Active").

(1) Select *Settings* > *Security* > *Users* and select the required user.

(2) Select the new status from the *Status* drop-down list: *Active, Dormant* or *Locked*.

(3) Select *Save*.

ELECTRONIC SIGNATURES & RECORDS

The system supports the use of electronic signatures and the creation of electronic records.

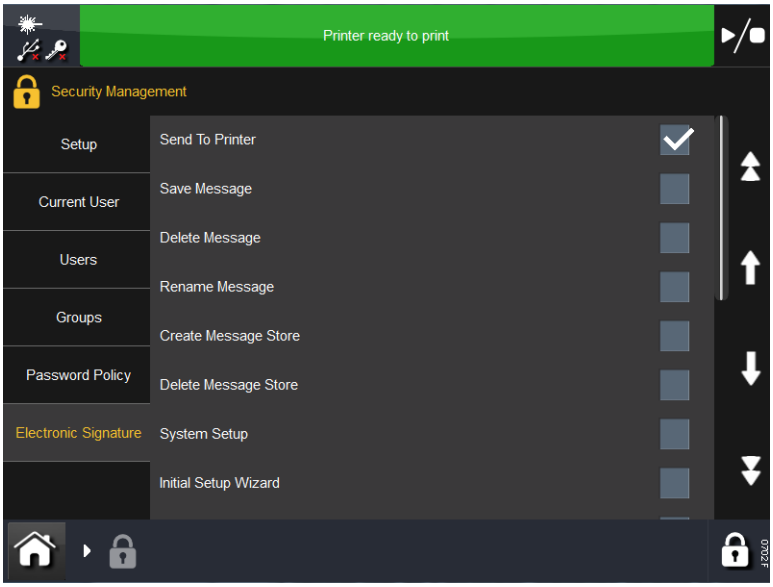
When users attempt to perform an action, which has been set as requiring an electronic signature, they will be required to enter their password (i.e. associate their user-id and password with the action) and in doing so, create an electronic record.

An Action Log is maintained that lists user actions; this log can be exported as a .db file.

Example

The following example demonstrates the electronic signature and records functionality.

(1) Login as 'Administrator' and select *Settings* > *Security* > *Electronic Signature.*



(2) Select the permissions for which an electronic signature will be required and select *OK*. In this example, the 'Send to Printer' permission has been selected.

(3) All users will now be required to enter their password before performing the action selected in the above list. This action, and its time and date, will then be logged against their name in the Audit Trail Log and will constitute an electronic record.

Note: *Any electronic signature options selected will apply to all users, including the Administrator.*

(4) Navigate to the Message Editor, create a new message and insert the text, 'MESSAGE ONE'.

(5) Save the message, with a name of your choice.

(6) Select *Send to Printer* and you will be required to enter your password; once entered the message will be sent to the printer. This action will be listed in the Audit Trial Log and is an electronic record.

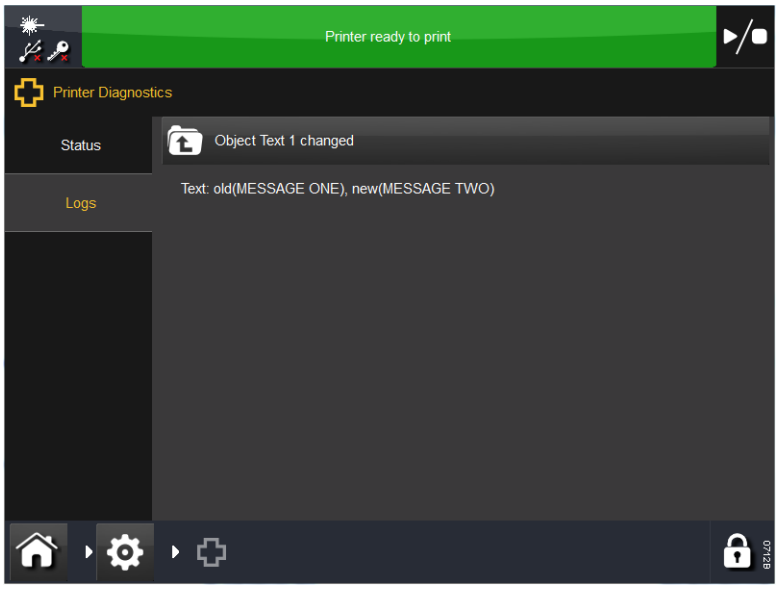
(7) Print the message several times.

(8) Edit the message, changing the text to ‘MESSAGE TWO’.

(9) Save the message and then send it to the printer, entering the password in the electronic signature dialog, as before. Print the message several times.

(10) Select *Settings* > *Diagnostics* > *Logs* > *Audit Trail Log*. This screen displays a list of actions, with the date and time of each action, the user id of the person who performed the action, and a description of the action.

(11) Select the ‘Object text 1 changed’ entry.



(12) The details of the change in text are displayed.

AUDIT TRAIL LOG

To optimise system performance, a daily archive is performed on the Action Log to move old records from the live database to the archive database.

The Audit Trail Log displays the 300 newest records plus any entries created since the last archive.

The Audit Trail Log can be exported at anytime, however, after the Log is, by default, 183 days old the user will not be able to enable marking until the Audit Trail Log is exported.

When the Audit Trail Log is, by default, 153 days old a warning message is displayed advising that the Audit Trail Log should be exported.

To change the number of days after which the warning and error messages are displayed select *Home* > *Settings* > *Alert Configuration* > *Ranged Alerts*.

To Export the Audit Trail Log

(1) Insert a USB memory device in one of the controller USB ports, or in the USB port of your means of remote access (e.g. Touchscreen panel).

(2) Select *Home* > *Settings* > *File Manager* > *PrinterDisk* > *Logs*.

(3) Select the Audit Trail Log 'Pencil' icon and select *Copy*.

(4) Select *File Manager* and then the relevant USB memory device.

(5) Select *Paste* to copy the log to the USB memory device.

The Audit log file (with file extension .log) will be listed on the USB memory device.

DOMINO DYN3LOGVIEWER

Once exported, the Domino Dyn3LogViewer utility, available on request from Domino, can be used to view the Audit Trail Log (live and archived records) on a standard MS Windows PC with .NET framework 3.5 installed.

The Dyn3LogViewer utility can also be used to export the Action Log to a text file.

To view the Audit Trail Log:

Open the Dyn3LogViewer utility and select *File* > *Open* and then select the required Audit Trail Log from its saved location.

The log entries language can be changed by selecting *Language* and selecting the required language from the drop-down list.

To export the Audit Trail Log as a text file:

Open the Dyn3LogViewer utility and select *File* > *Open* > *Export To Text File*, select the location in which you wish the file to be saved and press the *Save* button.

DELETING THE AUDIT TRAIL LOG

(1) Select *Settings* > *Diagnostics* > *Logs* > *Audit Trail Log.*

(2) Select the red  icon to view the ‘Delete entries older than (days)’ value. If required, edit the ‘number of days’ setting and select *OK*.