BellHawk®

Real-Time Operations Tracking and Management Software

www.BellHawk.com

BellHawk CFR Part 11 Capabilities User Manual

Introduction

The BellHawk Part 11 option, when enabled, adds features to a basic BellHawk inventory and production tracking system to ensure its compliance with the requirements of CFR 21 Part 11, which is required for validating a tracking system that is to be used in an FDA GMP environment.

These features are:

1. Ability to specify passwords for operators as well as for staff personnel.
2. Requesting a password as well as the employee badge number for each transaction performed on a shared device by operators.
3. Remembering a staff member’s badge number and password after they login on their own dedicated device so they do not have to repetitively enter these, when performing transactional data entry, provided that not more than a specified time has elapsed since they last used the device.
4. Requesting a password as well as the employee badge number for the first transaction performed on a non-shared (dedicated) device by an operator and then remembering the password as long as they continuously use the dedicated device. The password will be requested again if a specified time has elapsed without their using the device. It will also be requested if someone scans a badge on the device and it does not match the remembered password.
5. Allow the specification of the elapsed time for which passwords are remembered on dedicated devices.
6. Generate a daily audit log file of all data written to the database, with the time and date the information was written and who updated the database. This includes both setup and transactional data.
7. Enable downloading of the daily log files by date.

This document covers the changes added by the Part 11 capabilites. For other details, please see the appropriate BellHawk User’s Manuals, which it is assumed that the user had read before reading this manual.

These features are only available if the Part 11 option has been enabled.

For more details on the 21 CFR Part 11 compliance for this module, please see the Part 11 data sheet.

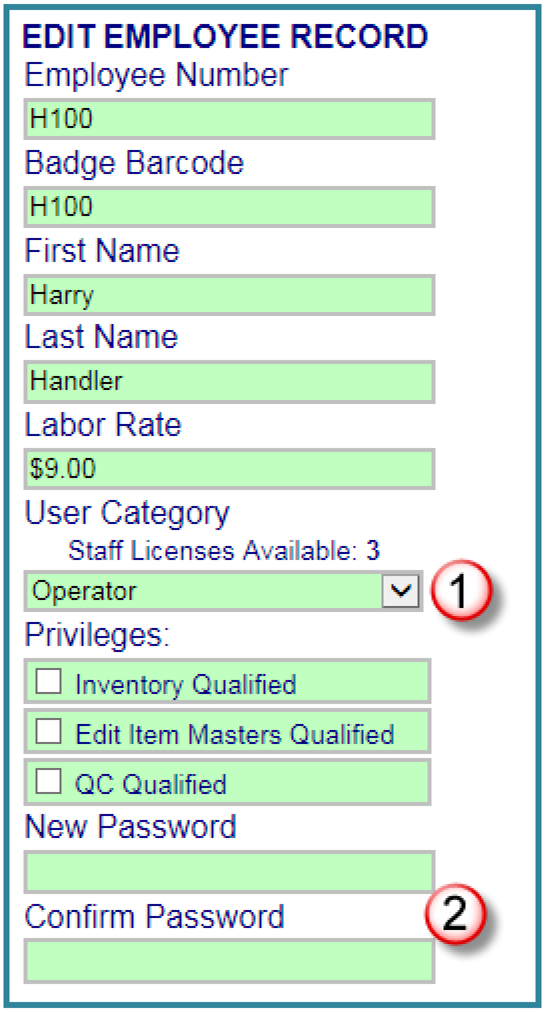
Table of Contents

Contents

Setting up Operator Passwords

When setting up employees, as shown at right, and you accept or select the User Category of Operator (1) then you will be requested to enter the password (2) for the operator being entered.

Note that, unlike Staff Members, Operators do not have User Names so they cannot login at the initial login screen in BellHawk, they have to use a device login.



EDIT EMPLOYEE RECORD

Employee Number: H100

Badge Barcode: H100

First Name: Harry

Last Name: Handler

Labor Rate: $9.00

User Category

Staff Licenses Available: 3

Operator

Privileges:

☐ Inventory Qualified

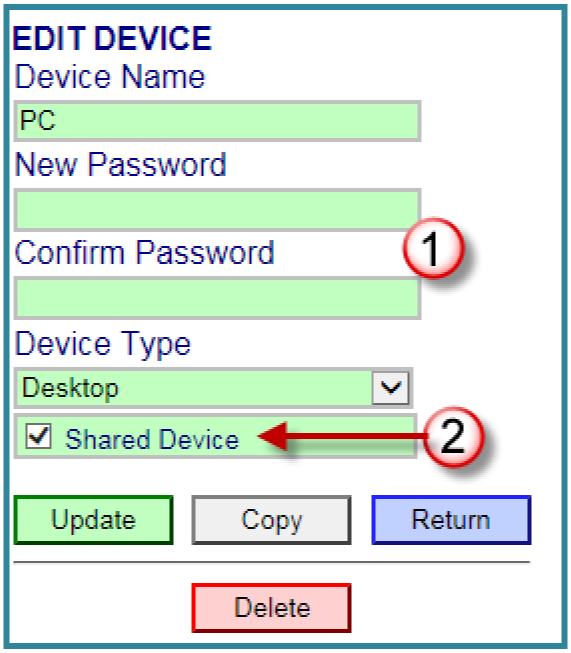
☐ Edit Item Masters Qualified

☐ QC Qualified

New Password:

Confirm Password:

Setting up Devices



EDIT DEVICE

Device Name: PC

New Password:

Confirm Password:

Device Type: Desktop

☑ Shared Device

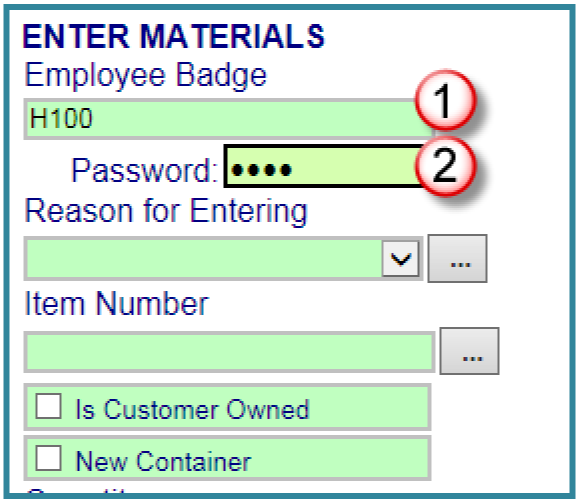
When setting up devices, the password you specify is for the device login, using the device name and password (1) on the main BellHawk login screen. All operators use devices, such as mobile computers, and do not have their own dedicated device logins.

You can set whether the device is shared or dedicated (2). On a shared device, an operator is expected to scan their badge and enter their password for every transaction. On a non-shared device they only have to scan their badge for each transaction as long as they use the device within a specified time of the last time they did a transaction.

Even if the password is remembered, if the badge does not match the remembered password then the password is requested again.

This dedicated device behavior can be beneficial to users of mobile devices, who typically use the same device for a shift. These devices have small keyboards and it is difficult to keep entering long passwords for every transaction. With shared PCs on a shop floor, it is essential to have the operators enter their passwords for every transaction.

Entering Passwords in Transactions



ENTER MATERIALS

Employee Badge: H100

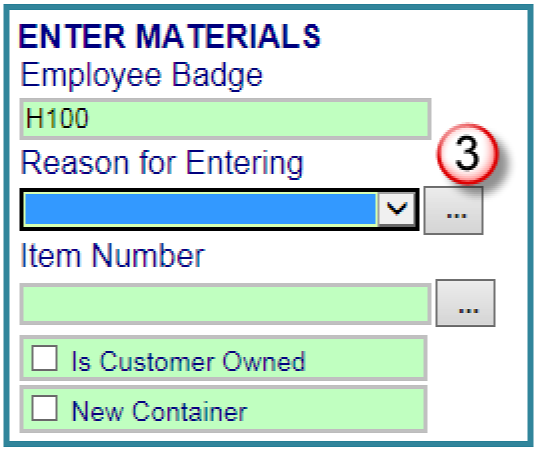
Password: ●●●●

Reason for Entering

Item Number

□ Is Customer Owned

□ New Container



ENTER MATERIALS

Employee Badge: H100

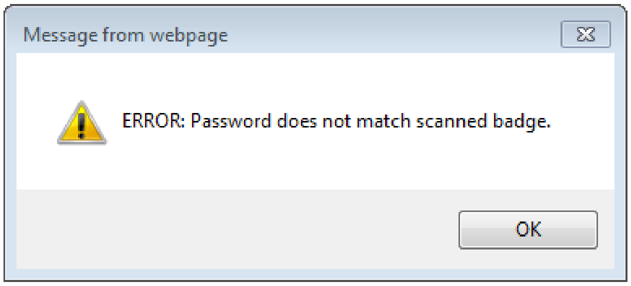
Reason for Entering

Item Number

□ Is Customer Owned

□ New Container

When Part11 is licensed and an operator enters their badge barcode number (1) –typically by scanning a barcode on their badge - then a Password (2) will be requested. This password must match the password for the operator having the scanned employee badge otherwise BellHawk generator a pop-up error warning, as shown here and does not allow the operator to submit any data until a correct password is entered.



Message from webpage

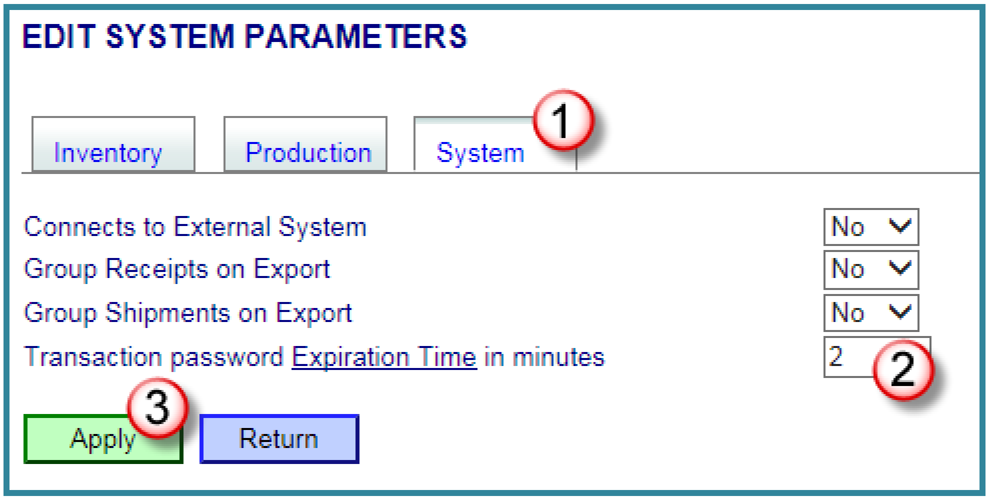
ERROR: Password does not match scanned badge.

Once a correct Password is entered the Password is made invisible (3) so as to maximize use of screen space for data entry on mobile devices.

As stated previously, on a dedicated non-shared device then a password is not requested from an operator or a staff member unless a specified amount of time has elapsed since the last transactional use of the device by the employee.

Setting the Elapsed Time

By default, the longest allowed time on a dedicated device before the password is requested again is 20 minutes. This can be set by a system administrator on the System Tab (1) of the Edit System Parameters screen, as shown here.



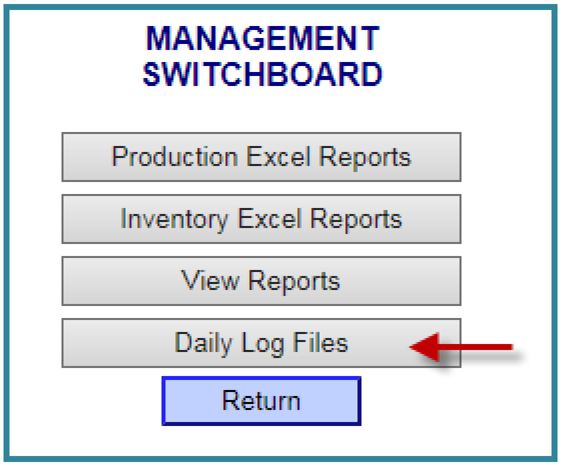
EDIT SYSTEM PARAMETERS

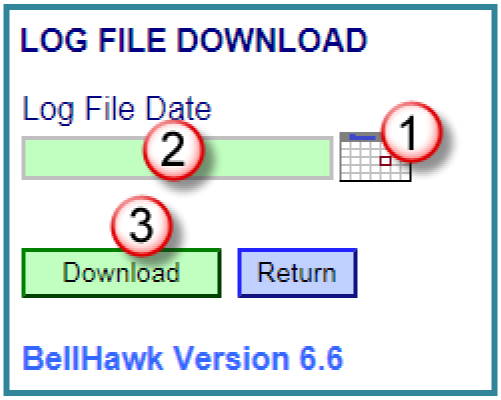
Connects to External System	No
Group Receipts on Export	No
Group Shipments on Export	No
Transaction password Expiration Time in minutes	2

If Part 11 is licensed the system's administrator will be able to set the password timeout (2) on shared devices. Please do not forget to select the Apply button (3) after entering your changes otherwise the value you entered will not be recorded.

Downloading the Daily Log Files

On the Management switchboard, you will see a button for Daily Log Files. Selecting this will bring up the screen below:


MANAGEMENT SWITCHBOARD


LOG FILE DOWNLOAD

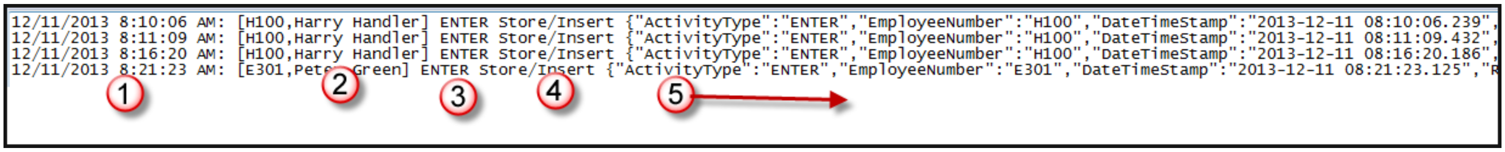
Log File Date

BellHawk Version 6.6

Select the date you want the log file for from the Calendar (1) or type it in (2) and then select the Download button (3). This will then ask you where you save the file (method dependent on the browser used). The file is downloaded as an ASCII text file, with a name that includes the date: `LogFile_20131211.txt`, for example.

This file can then be viewed with a text editor and printed out.

Format of Daily Log File



```
12/11/2013 8:10:06 AM: [H100,Harry Handler] ENTER Store/Insert {"ActivityType":"ENTER","EmployeeNumber":"H100","DateTimeStamp":"2013-12-11 08:10:06.239",
12/11/2013 8:11:09 AM: [H100,Harry Handler] ENTER Store/Insert {"ActivityType":"ENTER","EmployeeNumber":"H100","DateTimeStamp":"2013-12-11 08:11:09.432",
12/11/2013 8:16:20 AM: [H100,Harry Handler] ENTER Store/Insert {"ActivityType":"ENTER","EmployeeNumber":"H100","DateTimeStamp":"2013-12-11 08:16:20.186",
12/11/2013 8:21:23 AM: [E301,Pete Green] ENTER Store/Insert {"ActivityType":"ENTER","EmployeeNumber":"E301","DateTimeStamp":"2013-12-11 08:21:23.125","R
```

The daily log file contains the date and time of the data entry action (1), who performed it (2), the keyword of the business object being stored (3) and the action being performed (4) followed by the parameters of the data object in industry standard JSON format (5).

The JSON format represents the parameters of a business object as a sequence of “name” : “value” pairs separated by commas The data is presented at business object level so that it can be read and understood by non-programmers.

How the business object Keywords and Parameters names relate to the underlying data structures and stored procedures within the database can be viewed by a System Administrator using the DEXEL screens, as described in the Setup Users Manual and, by reference, the WebDexel User’s Manual.

This log file includes all updates made to the BellHawk database including those made through Excel imports, web-screen, and transactional data entry.

For changes to the log file made by the system administrator, the system will use the default e user name unless these are changed by the System Administrator to his own name.