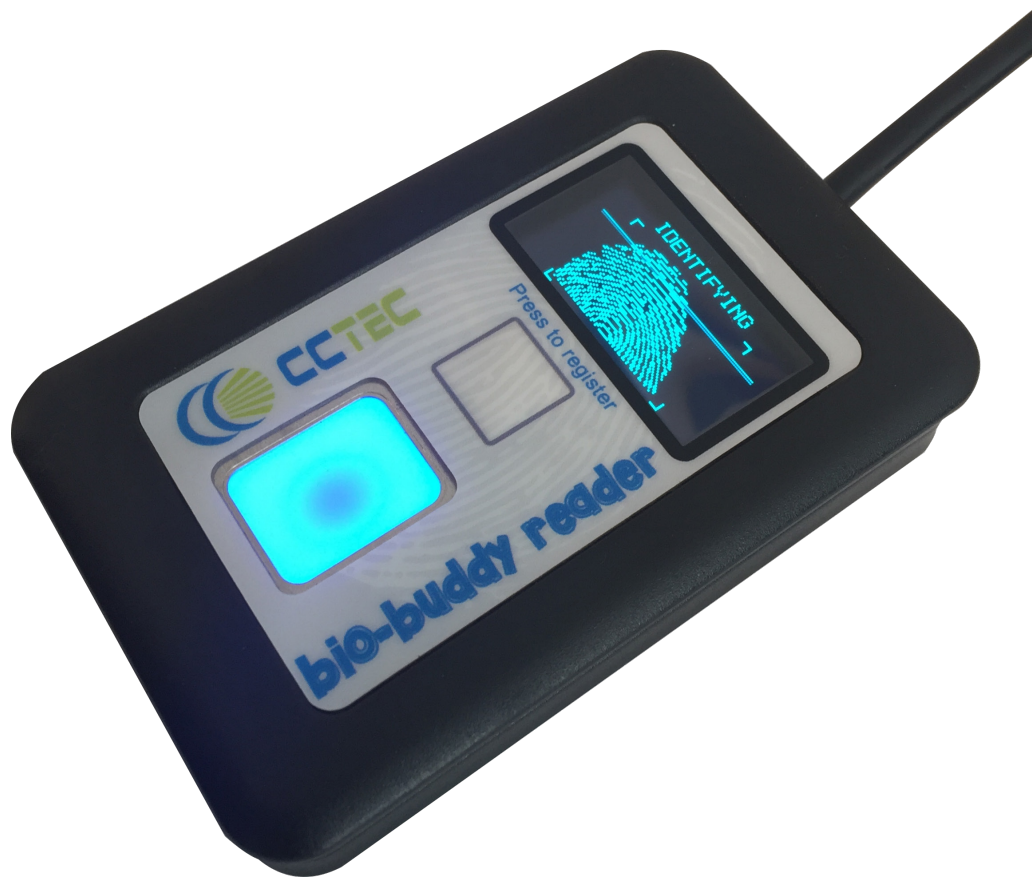


BIO-BUDDY READER



Introducing the Bio-Buddy Reader USB Biometric Terminal for PaperCut MF

The Bio-Buddy reader offers an incredibly low cost method for small organisations who wish to incorporate secure biometric identification on their multi-function devices, without the need for staff to be issued with PIN numbers or ID cards.

Cards can easily be lost, and PIN numbers forgotten, making the Bio-Buddy reader the perfect solution for secure identification at a price which won't break the bank.

With a simple software installation the Bio-Buddy reader easily connects via USB to an MFD. Alternatively, the Bio-Buddy reader can be connected to your network via a TCP converter.

How does it work?

The Bio-Buddy reader uses a process of self association and provides easy to follow instructions which guides the user through the process of self registration.

On first use of each reader the user simply presses the register button below the keypad and then places their finger on the keypad three times. This action registers the fingerprint in the reader and creates a unique number.

PaperCut MF then requests that the user enters their existing username and password on the embedded panel, CPad or release station to create the link and identify who the fingerprint belongs to.

Benefits at a glance

- Affordable method of secure authentication
- Compact size
- Simple to set-up with a plug and play style reader
- Users identify and authenticate themselves

Specifications

Box Dimensions:

- Length - 85 mm
- Width - 53 mm
- Height - 12 mm

Biometric Sensor:

- Central Processing Unit - ARM
- Sensor Type - Optical
- Image Size - 202 x 258 pixels
- Resolution - 450 dpi
- False acceptance rate: <0.001%
- Identification time - <1.0 seconds

Prerequisites

- Microsoft Windows 7 / 10 and Windows Server 2012 / 2016 Server
- Microsoft .NET Framework 4.5
- Microsoft SQL Server 2012 / 2014 / 2016 (including the free Express Editions)

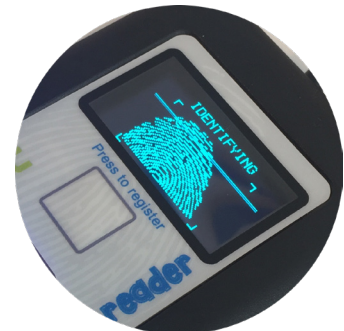
Step 1: Press registration button



Step 2: Place finger on scanner 3 times



Step 3: Fingerprint is registered and stored



Unknown users are flagged up on the display screen

