KEYWATCHER ACCESS CONTROL CHOICES EXPLAINED

The KeyWatcher comes standard with an alpha numeric 12-button keypad. Users enter a 4-digit user ID and a 4-digit PIN. Other available access methods are: hand reader, fingerprint, magnetic card swipe, bar code, and proximity reader. *Like a door to a building or room, the KeyWatcher stands by waiting for a valid signal from your preferred method of access validation.*

CARD ACCESS CONTROL TYPES

BAR CODE CARD READER

While any kind of card reader is more durable then biometric, bar codes are probably the least secure. Additionally, the bar code itself can be easily duplicated and is also subject to wearing off or scratching. The reader will also need periodic cleaning, which is easily accomplished using common cleaning pads.

MAGNETIC CARD SWIPE READER

This has been the most popular choice in card readers throughout the years. Just like your credit cards, the magnetic swipe eventually wears out and a new card will need to be issued. This gradual deterioration gives the user advanced warning and can then get it replaced before it completely fails. Like bar code card readers, the swipe card reader will also need periodic cleaning.

PROXIMITY CARD READER

No cleaning, no wear and tear, can't be copied…**this is definitely the most reliable interface with offering zero maintenance.** A user simply presents their card to within a few inches of the reader to login. Not much more to say.

COMMON TO CARD READERS

Card Readers are built into the KeyWatcher control panel. The card ID is stored seamlessly in the KeyWatcher and its' software. The card readers themselves are inexpensive choices. In most situations your existing cards and readers can also be used, or we can supply you with compatible readers and/or cards. We strongly recommend using a 4-digit PIN in conjunction with the access card of choice, so if a card is lost, it is unusable without the associated PIN number. The process would be to present the card and then enter a 4-digit PIN number. **Access issues are minimal with card readers.**

There are two methods for the readers to communicate to the KeyWatcher. The first method, which is also the most common, is when the reader is connected to the KeyWatcher and a valid read sends a signal directly to it as well granting access to its' menu. There is also a feature to disable the keypad until a valid card is read. Although rarely used the second method called, "relay input", is when the reader connects to an existing access control system. Upon a valid read the access control system sends a signal back to the KeyWatcher granting access to its' menu. This Relay Input method requires additional wiring between the KeyWatcher and your current access control panel.

BIOMETRIC ACCESS CONTROL

FINGERPRINT

Like card readers, fingerprint readers are built into the KeyWatcher control panel. Inexpensive compared to hand readers. Fingerprint readers are sensitive to wear and/or intentional/unintentional misuse. Fingerprint templates are seamlessly and effortlessly managed within the KeyPro software.

A user enters their 4-digit User ID on the KeyWatcher keypad and then places their finger when prompted for verification. With exception to the KeyWatcher administrators, once a Users fingerprint is enrolled, they cannot bypass the reader. As previously mentioned, fingerprint reader sensors are easily damaged, so you can count on replacing a sensor every one to two years depending on usage. Because the most common type of damage is sensor scratches, the replacement sensors are not covered under warranty.

HAND READER

Hand readers are mounted to the right of the main KeyWatcher cabinet. They require about 18 inches more wall space as well as their own network and ground connections. Hand readers are close to triple the price of fingerprint readers. There is also the additional cost of the HandNet software. While the hand reader is the most durable biometric interface offered, over time they will require internal cleaning and recalibration that must be done at the factory.

First, understand that hand readers are not palm readers. Hand readers take a geometric picture of the over 30,000 points of the top of your hand. There is only one manufacturer of hand readers in the world. A user enters their 4-10 digit User ID on the hand reader keypad and then places their hand when prompted. Like card readers, there is a feature to disable the KeyWatchers' keypad until a valid hand is read.

Secondly, a software package called HandNet that is separate from the KeyWatchers' KeyPro software, is required to manage templates. It stores a copy of the user hand template as well as constantly updating the hand template with normal changes in user hand such as gaining and losing weight. HandNet is a windows based Access Control program that communicates across the network to one or more readers via an optional Ethernet module. If the reader ever went down, you would just type the IP address in to the replacement reader and download the templates to it. HandNet is not networkable, meaning that multiple copies of the software cannot be installed and setup to share the same database. However, the hand reader(s) themselves can talk to the software via the network. **Hand readers are the only access control devices that require a separate software application.** Therefore, hand readers add an additional layer to the process of administering a KeyWatcher system. When you add a user to the KeyWatcher software you must also add them to the hand reader software.

HandNet software is also a great solution in that it can control numerous hand readers used for controlling access to various doors with electronic door strikes. Via access profiles you can control which readers a user can have access to. Each reader can have its' own network IP address and Ethernet card. It is being used in Vegas by several casinos to control both KeyWatchers and mantraps.

COMMON TO FINGERPRINT AND HAND READERS

Hand readers and fingerprint readers do need service over time. Fingerprint readers are the most sensitive component because of the sensor that the finger is placed upon. While hand readers need occasional recalibrating they seem to be more durable, but are not as integrated in to the KeyWatcher software as the fingerprint readers and your initial cost will be much higher. Regardless of what type of biometric access you choose we strongly encourage you to consider purchasing a spare.

DOCUMENT SUMMARY

If your application requires the level of security that biometrics provide, know that there is a tradeoff requiring higher upfront cost and maintenance. Access cards, such as swipe and proximity cards, run virtually problem free and are commonly already in place with most companies. *If our support team had their way, card access used in conjunction with a PIN number would be the only interface we would offer, as support on them is almost zero.*