NAC 708

Benutzerhandbuch

NovaCHRON Time & Access

biometric solutions

Haftungsausschluss

Änderungen an den in diesem Dokument enthaltenen vorbehalten. NovaCHRON übernimmt keine Haftung für direkte und indirekte, zufällige oder sonstige Schäden oder Folgeschäden, die aus dem Gebrauch oder durch die Verwendung der in dieser Benutzeranleitung enthaltenen Informationen entstehen.

Abbildungen von Bildschirmmasken, Listenausdrucken und sonstigen Auszügen innerhalb des Handbuchs spiegeln nicht notwendigerweise den aktuellsten Freigabestand wieder.

NovaCHRON Zeitsysteme GMBH & Co. KG
Agnetenstr. 14
39106 Magdeburg – Germany

Tel. +49 391 5410150
Fax +49 391 5410151

eMail: info@novachron.de
Internet: www.novachron-biometrics.com

INHALT

Vor dem Start

Wichtig zu wissen

Anmerkung: Bei auftretenden technischen Problemen versuchen Sie nicht das Gerät selbst zu reparieren, es sei denn, es wird in diesem Handbuch ausdrücklich empfohlen.

● Verwenden Sie Geräte mit optischem Fingerabdruckleser nicht an Plätzen mit starkem Lichteinfall. Dies kann einen signifikanten Einfluss auf den Scanvorgang des Fingerabdruckes haben und zu ungewollt schlechten Ergebnissen führen. Dieses Produkt ist für den Einsatz in Innenräumen konzipiert. Der Einsatz im Außenbereich erfolgt auf eigenes Risiko. und ist nicht von der Gewährleistung abgedeckt.

● Geräte zur Fingerabdruckerkennung sind komplizierte elektronische Maschinen, alle Sicherheitshinweise und Handbücher sollten vor einer Nutzung sorgfältig studiert werden.

● Die Produktgarantie deckt nicht Defekte oder Störungen ab, die durch fehlerhafte Installation, Benutzung, Lagerung und Transport ab sowie unautorisierte Serviceleistungen hervorgerufen wurden.

Das Enrollment und Identifikation von Fingerabdrücken sollten nach der Installation des Erfassungsgerätes vorgenommen werden.

Installation Enrollment Identifikation

Enrollment Installation Identifikation

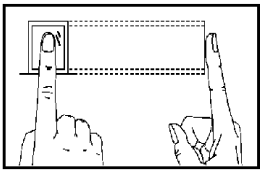
Die Erfassung des Fingerabdruckes

Für die Erfassung eines Fingerabdruckes sollte der zentrale Bereich eines Fingers verwendet werden. Legen Sie den deshalb so auf Oberfläche des Prismas, das dieser Bereich sicher erfasst werden kann.

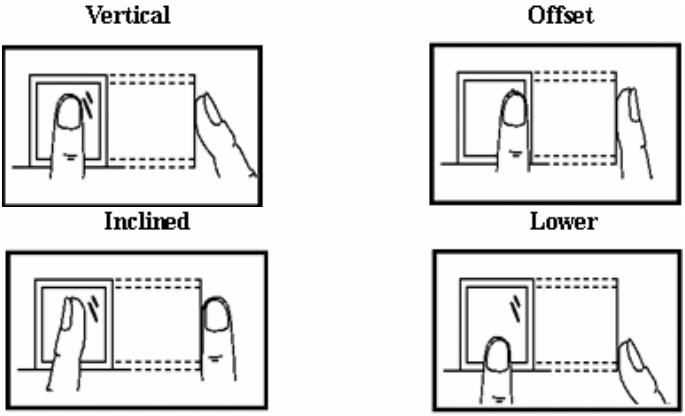
Um eine hohe Erfolgsrate zu erreichen, wird das Enrollment 3 mal wiederholt in einem jeweils leicht veränderten Winkel: Das erste Mal mit zentriert aufgelegtem Finger, der zweite Scan im Winkel leicht nach links und der dritte leicht im Winkel nach rechts.

Richtig:

Legen Sie den Finger flächig und zentral platziert mit leichtem Druck auf die Sensoroberfläche



Falsch:



Die Status-LEDs

Die Status-LEDs kennzeichnen in Abhängigkeit der Art des Blinkens unterschiedliche Arbeitszustände:

1. Grüne LED blinkt im Sekundenrhythmus – normaler Bereitschaftszustand
2. Fehlerhafte Autentizierung
   Rote LED leuchtet für 3 Sekunden
3. Verifikation erfolgreich
   Grüne LED leuchte für 3 Sekunden

Allgemeines

Dieser Abschnitt enthält Definitionen und Beschreibungen des Konzepts der Fingerabdruckerkennung mit Hilfe diese Erfassungssystems.

- User Enrollment
- User Verifikation
- Vergleichsschwellwerte
- User ID
- Privilege (Status) Levels

Die zwei wichtigsten Begriffe bei der Fingerabdruckerkennung sind das Enrollment und die Verifikation.

User Enrollment

Das Enrollment ist der Vorgang zur Erzeugung einer ID number und dem dreimaligen Scannen eines Fingers zur Erzeugung eines Templates. Diese Template wird mit der User-ID verbunden und abgespeichert.

Nun kann das abgespeicherte Fingerabdruckreferenz-Template verglichen werden mit dem Template, erzeugt aus dem Fingerabdruck eines aufgelegten Fingers.

Durch den Vergleich des abgespeicherten Templates mit dem

aktuell durch den Benutzer erzeugten kann die Identität des überprüft werden und seine Berechtigung eine Zeitbuchung mit dieser Identität zu erzeugen. Der gesamte Vorgang dauert weniger als 2 Sekunden. Für die gleiche User-ID können bis zu 10 Finger eingescannt werden. Idealerweise sollten zumindest mehr als ein Finger enrolled werden, um im Problemfall einen alternativen Finger nutzen zu können. Dazu sollten der linke und rechte Zeigefinger benutzt werden. Dies gestattet die Verwendung eines alternativen Fingers und gleichzeitig kann nicht vergessen werden, welcher erfasst ist.

Identifikation/Verifikation

Bei der Verwendung biometrischer Systeme zur Authentifizierung von Personen stößt man immer wieder auf die Begriffe Identifikation und Verifikation. Ziel einer biometrischen Erkennung ist stets, die Identität einer Person zu ermitteln (*Identifikation*) oder eine behauptete Identität zu bestätigen bzw. zu widerlegen (*Verifikation*).

Bei einer **Identifikation** wird *ein* biometrische Merkmal mit *allen* im System gespeicherten Referenzmerkmalen verglichen (1:n Vergleich). Gibt es eine Übereinstimmung, ist die Identifikation erfolgreich und die zum betreffenden Referenzmerkmal gehörende User-ID lässt sich weiterverarbeiten.

Bei einer **Verifikation** gibt der Nutzer dem System seine Identität vorab bekannt (z. B. über eine PIN oder Karte), das System muss das biometrische Merkmal dann nur noch mit *einem* zur User-ID passenden Referenzmerkmal (1:1 Vergleich) vergleichen. Im

Übereinstimmungsfall ist die Verifikation erfolgreich.

Vergleichsschwelle

Die Vergleichschwelle ist eine Zahl, welche den Grad der Übereinstimmung zwischen der erfassten und dem abgespeicherten Template.

Die Erfassung und Auswertung biometrischer Merkmale ist naturgemäß mit Messfehlern behaftet, da sich die verwendeten Merkmale sowohl im Laufe der Zeit als auch temporär durch äußere Einflüsse ändern und auch die Präsentation gegenüber dem System niemals gleich erfolgt. Die zu unterschiedlichen Zeitpunkten erzeugten digitalen Abbilder des gleichen biometrischen Merkmals können also nicht zu 100% identisch sein. Es erfolgt also beim Matching deshalb keine Überprüfung auf Gleichheit sondern auf hinreichende Ähnlichkeit.

Die Falsch-Zurückweisungsrate (FRR)

Die FRR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der berechtigte Personen unberechtigterweise zurückgewiesen werden. Die FRR ist in der Regel ein Komfortmerkmal, da falsche Abweisungen vor allem lästig sind aber die Sicherheit nicht beeinträchtigen.

Die Falschakzeptanzrate (FAR)

Die FAR ist die Häufigkeit (ausgedrückt als prozentualer Anteil), mit der nicht berechtigte Personen als berechtigt akzeptiert

werden. Da eine falsche Akzeptanz in der Regel zu Schäden führt, ist die FAR ein sicherheitsrelevantes Maß. Die FAR wird allgemein als wichtigstes Kriterium für die Qualität einer Biometrielösung angesehen. Beide Werte können durch Änderung der Vergleichsschwelle innerhalb des Systems beeinflusst werden, stehen jedoch immer in direkter Abhängigkeit zueinander: eine Verringerung der FAR führt unmittelbar zu einer Erhöhung der FRR und umgekehrt. Die Vergleichsschwelle kann für alle Benutzer eingestellt werden. Für einen Benutzer dessen Fingerabdruckerkennung schwierig kann zur Verifikation gewechselt werden: ID + Fingerabdruck (1:1 Vergleich). Eine Erhöhung der Toleranzschwelle erhöht die Sicherheit – eine Absenkung hingegen erhöht ungewollten Zugang. Deshalb ist die richtige Balance zwischen beiden Werten wichtig.

Anmerkung: FAR und FRR beeinflussen einander, eine Erhöhung der FAR führt zur Reduzierung der FRR. Der Default-Wert für die Tolleranzschwelle ist 35, bei 1:1 Vergleich 15.

Tabelle 1—1 Empfohlene Schwellwerte

FRR	FAR	1:1	1:n
hoch	niedrig	45	25
mittel	mittel	35	15
niedrig	hoch	25	10

User-ID

Bevor das Enrollment beginnt, wird dem Benutzer eine ID zugeordnet. Diese User-ID wird benötigt um ein Fingerabdruck-Template oder Passwort im Verifikationsmodus aufzurufen.
Die ID wird über die Tastatur eingegeben.

Berechtigungen

Über das Administrator Menü werden die Berechtigungen von Benutzern zum System eingestellt und verwaltet.

Es können vier verschiedene Stufen zugeordnet werden:

- Benutzer – nur mit der Berechtigung sich zu registrieren und Zeit- oder Zutrittsbuchungen zu erzeugen
- Enroller – mit der Berechtigung andere Benutzer zu enrollen oder zu löschen
- Administrator – Systemverwaltung mit Ausnahme der erweiterten Optionen
- Supervisor – verfügt über alle Berechtigungen

Anmerkung: Ist kein Administrator oder Supervisor im System vorhanden, kann ein Administrator vom Enroller angelegt werden. Ist kein Supervisor im System, kann dieser vom Administrator angelegt werden.

Erste Schritte

Dieses Kapitel beschreibt das Enrollment und die Verifikation der Benutzer im Fingerabdruck-Identifikationssystem.

- Benutzer-Enrollment
- Testen eines Enrollments
- Enrollment von weiteren Fingerabdrücken
- Verifikation einer Identität
- Hinweise für erfolgreiches Enrollmemt
- Benutzer-Enrollment

Benutzer-Enrollment

Nach dem durchgeführten Setup des Gerätes und dem Anschluss an die Stromversorgung kann das Enrollment der Benutzer durchgeführt werden. Ist dies das erste Enrollment in einem neuem System ist jeder Benutzer zum Enrollment berechtigt. Ist bereits ein Administrator im System vorhanden kann das Enrollment von diesem oder einer von ihm berechtigten Person durchgeführt werden. Diese Gerät bietet 3 Möglichkeiten des Enrollments an: das Fingerabdruck-Enrollment, das Passwort-Enrollment sowie das Fingerabdruck und Passwort-Enrollment. Diese drei Arten können Personen mit unterschiedlicher Qualität des Fingerabdruckes individuell zugeordnet werden. Das

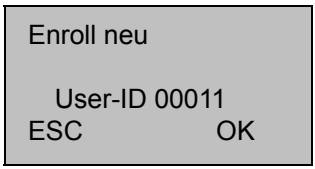
Fingerabdruck-Enrollment ist geeignet für Personen, deren Fingerabdruckqualität gut ist, das Fingerabdruck und Passwort – Enrollment ist geeignet für Personen, deren Fingerabdruck sich enrollen lässt, aber die Verifikation manchmal schwierig ist, das Passort-Enrollment sollte für Personen verwendet werden, bei denen das Enrollment bereits schwierig ist. In Abhäbgigkeit von der jeweiligen Situationen sollte stets die geeignete Art des Enrollments gewählt werden.

Um das Enrollment-Vorgang zu beginnen, drücken Sie die Menü-Taste, geben sie Ihre ID-Nummer oder Fingerabdruck ein, damit Ihre Identität überprüft wird.

Anmerkung: Ist dies das erste Enrollment in einem neuen oder leerem System, wird nach dem Drücken der Menü-Taste keine Verifikation durchgeführt.

Fingerabdruck Enrollment

1. Drücken Sie die Menü-Taste und wählen Sie das Menü **User-Verwalt.\ Enroll User\Enroll FP\Enroll neu**. Sie sehen die folgende Anzeige:



2. Geben Sie die User-ID ein (Bereich von 1 to 65534), drücken Sie [OK],

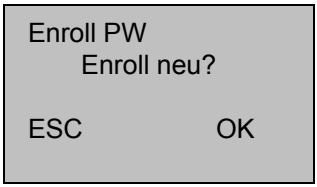
3. Mit dem nachfolgenden Bildschirm werden Sie aufgefordert, einen Finger dreimal auf die Sensoroberfläche zum Scannen aufzulegen.

Anmerkung: 00011-0 Die letzte Ziffer 0 bedeutet Fingerabdruck

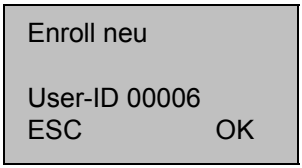
4. Nach Beendigung des Scanvorganges bestätigen Sie mit OK das Speichern des Templates. Sollte der Scanvorgang nicht erfolgreich sein, werden Sie zur Wiederholung aufgefordert.

Passwort Enrollment

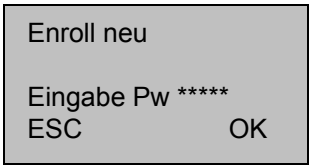
1. Betätigen Sie den Menü-Button um in die User-Verwaltung zu gelangen und wählen Sie anschließend Enrollment PW, drücken Sie die [OK], der folgende Bildschirm wird angezeigt::



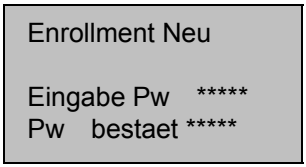
2. Drücken Sie [OK], der folgende Bildschirm wird angezeigt:



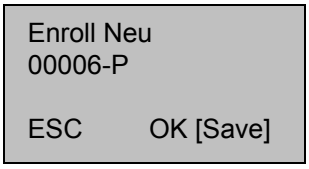
3. Geben Sie die User–ID ein (im Bereich von 1 bis 65534), drücken Sie [OK]:



4. Geben Sie das Passwort ein:



5. Geben Sie das Passwort zur Kontrolle nochmals ein und drücken Sie [OK]:

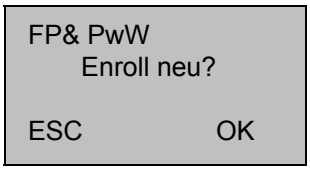


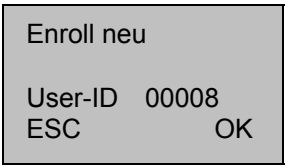
Anmerkung:00006-P Der Buchsabe P steht für Passwort.

6. Drücken Sie [OK] zur Speicherung des Passwortes.

Fingerprint & Passwort

1. Drücken Sie die Menütaste um in die User-Verwaltung zugelangen. Wählen Sie Fingerprint und Passwort (FP&PW):

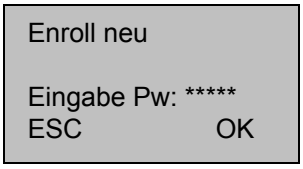




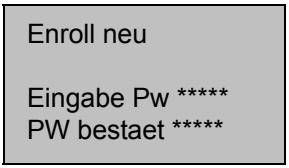
2. Drücken Sie [OK]:

3. Geben Sie die User-ID ein (Bereich 1 bis 65534) und drücken Sie [OK]:

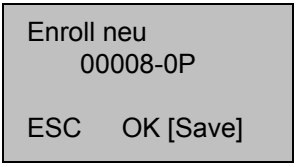
4. Nachdem erfolgreichen dreimaligen Scanvorgang wird folgender Bildschirm angezeigt:



5. Geben Sie Ihr Passwort ein:



6. Geben Sie Ihr Passwort zur Überprüfung nochmals ein und drücken Sie [OK]:

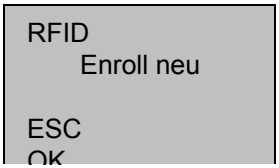


Anmerkung: 00008-0P; Die Ziffer 0 steht für Fingerprint und P für Passwort.

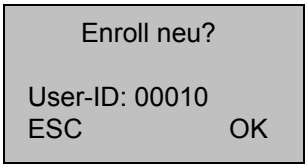
7. Drücken Sie [OK] zur Speicherung der Daten.

Enroll RFID (Option)

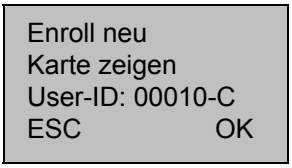
1. Drücken Sie die Menü-Taste um in die User-Verwaltung zu gelangen. Wählen Sie RFID und drücken Sie [OK]:



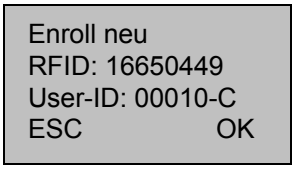
2. Drücken Sie [OK]:



3. Geben Sie die User-ID ein (Bereich 1 bis 65534) und drücken Sie [OK]:



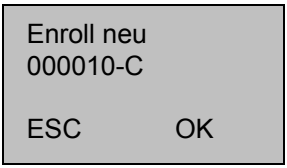
4. Halten Sie die Karte vor den Leser. Die Karte wird ausgelesen und der User–ID zugeordnet:



Anmerkung: 00010-C Der Buchstabe C steht für Karte

5. Drücken Sie [OK] um die erfassten Daten zu akzeptieren.

6. Sie können nun Erfassungsvorgang mit der Taste ‘ESC’ abzubrechen. Durch Drücken der Taste **OK** werden die Daten



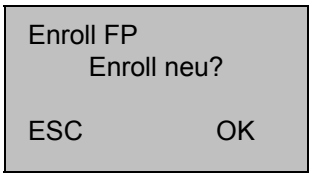
abgespeichert und der Registrierungsvorgang der ID-Karte abgeschlossen.

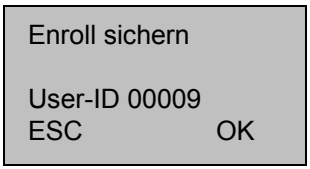
Testen auf erfolgreiches Enrollment

Fordern Sie den Nutzer auf, den Finger auf der Sensoroberfläche zu platzieren, um eine die Qualität der Verifikation zu überprüfen. Ist dieser Test erfolgreich, können Sie diesem Nutzer für die Erfassung die Fingerabdruck-Identifikation zuweisen. Anderenfalls wird empfohlen die Verifikationsmethode mit Fingerprint + Passwort zu verwenden.

Enrollen von zusätzlichen Fingerprints für einen Nutzer

Für eine langfristige Nutzung, wenn es der Systemspeicher erlaubt, wird die Erfassung von mehr als zwei Fingerprints empfohlen. Wechseln Sie hierfür in das Menü **Enroll User\Enroll FP**. Drücken Sie die **OK** Taste um das User Enrollment weiterzuführen. Drücken Sie 'ESC' um ein neues Enrollment abzubrechen und in das Backup-Enrollment zu gelangen:





Der Ablauf ist der Gleiche wie bereits oben beschrieben für das Enrollen eines neuen Nutzers.

Autentikationsarten

Fingerabdruck Autentikation

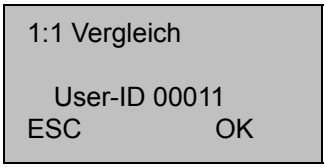
Für die Nutzung von Fingerabdrücken zur Mitarbeiteridentifikation stehen verschiedene Autentifikationsarten zur Verfügung:

1. Der 1:1 Vergleich - Verifikation

In diesem Modus wird gibt sich der Nutzer vor dem Einscannen des Fingers durch Eingabe einer ID, die einem bereits registrierten Fingerabdruck zugeordnet ist, zu erkennen. Dieser registrierte Fingerabdruck wird nun mit dem eingegebenen Fingerabdruck verglichen. Die 1:1 Autentikation benötigt eine kürzere Zeit als ein Vergleich gegen alle im System gespeicherten Templates. Um den 1:1 Vergleich zu nutzen sind keine speziellen Einstellungen im System erforderlich. Nach der Eingabe der ID wird automatisch ein 1:1 Vergleich durchgeführt.

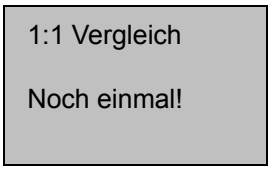
Durchführung

Geben Sie Ihre User-ID ein:



Drücken Sie **OK** und legen Sie den Finger auf die Sensoroberfläche. Der Abgleich dauert etwa 0,5 Sekunden. Ist dieser erfolgreich, erfolgt eine akustische Quittierung.

Konnte Ihre Identität nicht bestätigt warden, erfolgt eine Aufforderung zur Wiederholung des Vorganges:



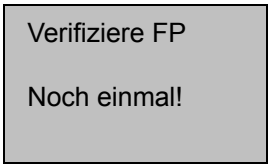
2. 1:n Vergleich - Identifikation

Alle erfassten Fingerabdruck-Templates können für die 1:n Autenfikation verwendet werden. Diese Art der Authentifizierung ist für den Nutzer sehr einfach, erfordert etwas mehr Zeit als die 1:1-Identifikation da gegen alle gespeicherten Templates verglichen wird. Für die Nutzung dieser Autentifikationsart sind keine speziellen Einstellungen im System erforderlich.

Durchführung

Legen Sie den Finger auf die Sensoroberfläche. Der Abgleich dauert etwa 0,5 - 2 Sekunden. Ist dieser erfolgreich, erfolgt eine akustische Quittierung.

Konnte Ihre Identität nicht bestätigt werden, erfolgt eine Aufforderung zur Wiederholung des Vorganges:



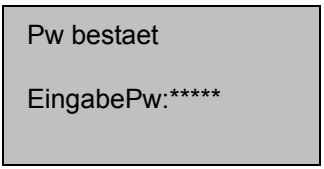
Passwort Autentifikation

Ein Passwort bestehend aus 1--5 Ziffern kann ebenfalls zur Autentifikation verwendet werden. Dies kann in den Fällen zum Einsatz kommen, wenn die Qualität der Fingerabdrücke für eine Fingerprint-Autentifikation ungeeignet ist.

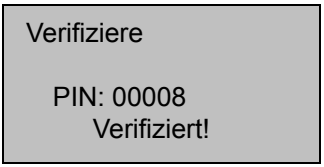
Durchführung

Geben Sie Ihre ID ein:

Drücken Sie [OK]:



Geben Sie Ihr Passwort ein und drücken Sie [OK]:



Empfehlungen für erfolgreiches Enrollment

Weist der Fingerabdruck oder besser das daraus extrahierte Template eine gute Qualität auf, so wird die Verifikationsgeschwindigkeit sehr hoch sein. Anderenfalls sinkt die Verifikationsgeschwindigkeit oder es werden Nutzer als nicht berechtigt zurückgewiesen. Nachfolgend erhalten Sie einige

Hinweise zur Problembehandlung:

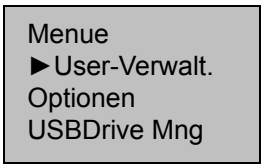
Problem	Lösung
Finger ist zu trocken oder schmutzig	Säubern Sie den Finger. Erhöhen Sie Feuchtigkeit der Hautoberfläche (Anhauchen)
Zu wenig Druck beim Auflegen	Der Nutzer sollte den Finger flach und mit leichtem Druck auf die Sensoroberfläche auflegen
Welcher Finger sollte benutzt werden?	Empfohlen wird der rechte oder linke Zeigefinger oder Mittelfinger. Benutzen Sie Fingerabdrücke von guter Qualität ohne sichtbare Verletzung oder andere Einschränkungen. Normalerweise sollte der Zeigefinger benutzt werden. Ist der Abdruck dieses Fingers von schlechter Qualität, sollte der Mittel- oder Ringfinger genutzt werden. Ist der Finger des Nutzers zu klein, wird der Daumen empfohlen.
Wie ist der Finger zu platzieren?	Legen Sie den Finger flach und zentriert mit leichtem Druck auf. Die Sensoroberfläche soll mindestens zu mehr als 2/3 bedeckt sein. Vermeiden Sie ein seitliches Auflegen. Warten Sie bis der Scanvorgang beendet ist bevor Sie den Finger entfernen. Bewegen Sie den

	Finger nicht auf der Sensoroberfläche während des Scannens.
Andere	Es gibt einige Menschen deren biometrische Merkmale wenig ausgeprägt sind. Deren Fingerabdrücke können zu Problemen bei der Erfassung führen. Wechseln Sie in diesem Fall zur Verifikationsmethode mit ID + Fingerprint oder nutzen Sie die Passwort Verifikation bzw. die Verifikation per ID-Karte. Eine weitere Lösung ist die Reduzierung der Toleranzschwelle.

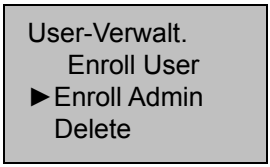
Administrator Enrollment

Um zu verhindern, dass unbefugtes Personal Manipulationen im System vornimmt, können Sie Administratoren mit unterschiedlichen Berechtigungen anlegen.

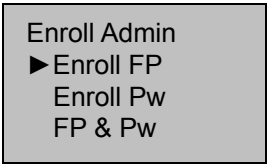
1. Drücken Sie die Menü-Taste des Gerätes:



2. Wählen Sie das Menü für die User-Verwaltung und mit der Taste ▼ das Menü **Enroll Admin**:



3. Drücken Sie **OK** und wechseln Sie in das Menü zum Fingerprint Enrollment:



4. Sie können nun die gewünschte Art des Administrators auswählen:

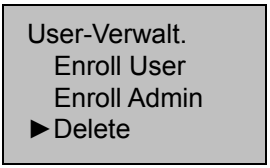
- Enroller
- Administrator mit Enroller-Berechtigung
- Supervisor

Die Art des Enrollments ist die gleiche wie beim User-Enrollment.

Nach dem Anlegen eines Administrators ist der Zugang zur Menüstruktur nur nach einer Autorisierung erlaubt.

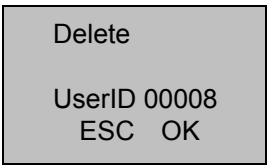
Löschen von Nutzern

1. Drücken Sie Menü und wechseln Sie in die User-Verwaltung.
2. Mit Hilfe der "▲/▼" Tasten auf den Punkt **Delete** navigieren



3. Mit **OK** in das Untermenü verzweigen

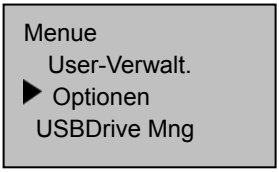
4. Geben Sie die User-ID ein, der zu löschenden Person und drücken Sie OK, um zu bestätigen. Drücken Sie jeweils OK,



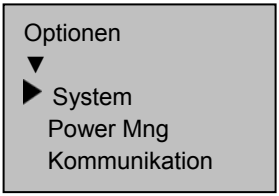
damit die einzelnen zugeordneten Benutzerinformationen aus dem Terminal entfernt werden.

Optionen

Drücken Sie die Menü-Taste und identifizieren sich, damit folgendes Menü erscheint:



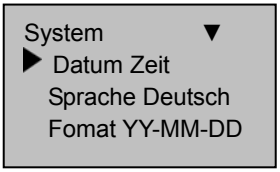
Wählen Sie Optionen und bestätigen Sie dies mit OK.



Der folgende Abschnitt beinhaltet die System-Optionen, das Power-Management, Kommunikationsparameter, Log-Optionen und den Auto-Test des Terminals.

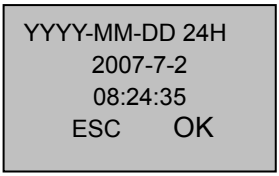
System

Wählen Sie im Menü die Systemoptionen:



Datum Uhrzeit

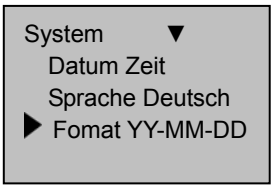
Zum Einstellen von Datum und Uhrzeit am Terminal verzweigen sie in das Menü ***Datum Zeit***.



Geben Sie das korrekte Datum sowie die korrekte Zeit ein und schließen sie die Eingabe mit **OK** ab.

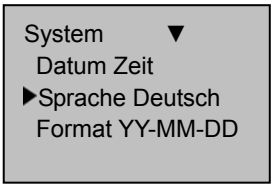
Format für die Darstellung von Datum und Uhrzeit

Wählen Sie im Menü **System\Optionen** den Menüpunkt Format an. Selektieren Sie das gewünschte Datumsformat z. B. DD.MM.YY und bestätigen Sie mit ***OK***. Anschließend haben Sie die Möglichkeit, zwischen verschiedenen Anzeigenformaten über die Pfeiltasten zu wechseln.
Wählen Sie das entsprechende Format aus und bestätigen Sie dies mit ***OK***.



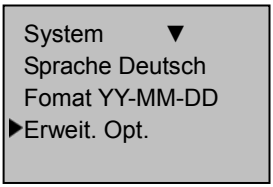
Wechseln der Terminalsprache

Wählen Sie im Menü **Optionen\System** den Menüpunkt **Sprache** an. Über die Pfeiltasten können Sie zwischen deutscher und englischer Sprache wechseln. Schließen Sie ihre Änderung mit **OK** ab. Anschließend **Esc** drücken, um das System-Menü zu verlassen und die Änderungen mit **OK** abspeichern. Das Terminal muss neu gestartet werden, damit die Sprachänderungen sichtbar werden.



Erweiterte Optionen

Wechseln Sie in das Menü **Optionen\System** und selektieren Sie den Punkt **Erweit. Opt.** und bestätigen Sie mit OK:



Über die "▲/▼" Tasten können sie zwischen den einzelnen Menüpunkten wechseln und die einzelnen Optionen auswählen:

- **Reset Optionen:** Zuücksetzen der Optionen auf die Standard-Werte.
- **Loesch AnwLogs**: Löscht alle Benutzer und Bewegungsdaten
- **Loe. alle Daten**: Löscht alle Daten im Terminal
- **AdmRechte loes:** Administratoren-Rechte löschen
- **Show Score**: Zeigt die erreichte Schwelle an, wenn die Toleranzschwelle unterschritten wurde
- **VerglSchwell 35** Einstellung der Vergleichs- oder Toleranzschwelle für 1:n-Vergleich
- **Eingabe ID N** Umstellung auf Verifikationsmodus des Terminal
- **1:1 Schwelle** Einstellung der Vergleichs- oder Toleranzschwelle für 1:1 Vergleich
- **Sprache**: Sprachausgabe ein-/auschalten
- **Upd Firmware** Firmware-Update über USB-Port ausführen
- **Remote Auth** Option

- **AuthSever IP** Option
- **Tastatur Piep:** Ein-/Ausschalten des Quittierungstons bei Tastaturbedienung

5

Kommunikation

Verzweigen Sie in das Menü **Optionen \ Kommunikation**, um die Einstellungen für die Datenübertragung zwischen Host und Terminal vorzunehmen.

Das Gerät unterstützt **RS232, RS485** und **TCP/IP**.

- **IP-Adresse:** Standard-IP-Adresse ist die 192.168.1.201. Geben Sie die gewünschte IP-Adresse ein
- **Net Mask**: Standard-Netzwerk-Maske ist die 255.255.255.0
- **Gateway:** Bei Bedarf können sie an dieser Stelle die Gateway-Adresse ihres Netzwerkes eingeben.
- **Netz-Geschwindigkeit:** Standard-Wert ist Auto. Weitere Optionen sind 10M-F, 10M-H, 100M-F, 100M-H
- **Baud Rate:** 5 Baudraten können gewählt werden: 9600, 19200 38400, 57600 115200;

- **Geräte-Nummer**: Hier geben sie die Geräte-Nummer des Terminals vor. Standard ist die 1 und ist nur bei Benutzung innerhalb eines RS485-Netzwerkes mit mehreren Terminals zu ändern. Achten sie darauf, dass alle Terminals im RS485-Netzwerk unterschiedliche Adressen haben, ansonsten führt die Kommunikation zu Fehlern.
- **RS232:** Ein-/Ausschalten der RS232-Schnittstelle
- **RS485:** Ein-/Ausschalten der RS485-Schnittstelle
- **Komm-Pw:** Standard-Wert ist die 0

Nach dem Ändern der Kommunikations-Optionen muss das Gerät neu gestartet werden!

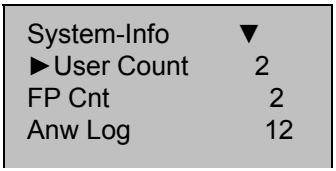
Auto-Test

Über den Auto-Test können sie die einzelnen Komponenten des Gerätes überprüfen. Wechseln sie in das entsprechende Menü und sie erhalten Zugriff auf die einzelnen Tests, wie **Speicher**, **LCD, Fingerprint-Sensor**, **Tastatur .**

System Informationen

Zur Anzeige der Geräte-Informationen verzweigen sie im Hauptmenü in das Menü **System-Info**.

Anschließend werden ihnen verschieden Informationen über den Geräte-Status angezeigt.



- **User Count**: Anzahl der angelegten Nutzer
- **FP Cnt**: Anzahl der hinterlegten Fingerprints
- **AnwLog** : Anzahl der gespeicherten Buchungs-Datensätze
- **Admin Cnt**: Anzahl der registrierten Administratoren
- **User Pw** Anzahl der Nutzer, die ein Password zur Identifikation nutzen.
- **Supv Log**: Supervisor Datensätze
- **Freier Speicher**: verfügbarer freier Speicher im System
- **Geräte-Info**: Information über das Gerät
- **Firmware**: Firmware-Stand

- **Algversion**: Version Fingerprintalgorithmus
- **Serien-Nummer**: Geräte-Serien-Nummer.

Reinigung

In bestimmten Zeitabständen sollte eine Reinigung von Geräteoberfläche, Tastatur, Display und Sensoroberfläche erfolgen. Wegen der unterschiedlichen Umgebungsbedingungen sind jedoch allgemeine Empfehlungen für die Zeitabstände nicht möglich. Beachten Sie deshalb die nachfolgenden Hinweise:

Geräteteil	Reinigungsabstände
Tastatur und Display	Eine Reinigung ist erforderlich, wenn die Sichtbarkeit des Displays nachlässt.
Optischer Sensor	Die Sensoroberfläche ist ausgelegt für den Betrieb unter schmutzigen Bedingungen. Sie sollte nicht zu häufig gereinigt werden.
	Eine Reinigung sollte vorgenommen werden, wenn eine abnehmende Lesesicherheit beobachtet wird.

Reinigung von Tastatur und Display

Benutzen Sie zur Reinigung solche Produkte wie zur Reinigung von Monitoroberflächen.

Reinigung des optischen Sensors

Die Reinigung der Oberfläche des optischen Sensors sollte wie nachfolgend beschrieben vorgenommen werden:

(1) Entfernen Sie mit Staub und lose anhaftende Partikel von der Oberfläche ab.

(2) Benutzen Sie hierzu ein Klebeband wie Tesafilm oder Ähnliches.

(3) Benutzen Sie ein nicht fusselndes, weiches und trockenes Tuch. Gehen Sie sorgfältig vor, um die Sensoroberfläche nicht zu zerkratzen.

Achtung:

Benutzen Sie keinerlei Reinigungsmittel oder Lösungsmittel, die Sensoroberfläche kann dadurch nachhaltig beschädigt werden.

NovaCHRON Zeitsysteme GmbH & Co KG
Agnetenstraße 14
39106 Magdeburg

Tel.: +49 391 5410150
Fax: +49 391 5410151

eMail: info@novachron.com
www.novachron-biometrics.com

NovaCHRON
Time & Access
biometric solutions