Protect Master

Konfigurationshandbuch

TwinLock ProtectMaster IP (7220 / 7260)

VdS

VdS 2396 nach EN 1300

G105133	Schalteinrichtung (VdS Klasse C)
G108062	Überfallmelder (VdS Klasse C)
G106016	Sperreinrichtung (VdS Klasse C)
G108061	Überfallmelder (VdS Klasse C)

Business Plattform

M109316	TwinLock 7260 Plattform
M109318	TwinLock 7220 Plattform

TwinLock Protect Master | Das IP-Schloss

Version: 2.1.7
Anleitung: 1.4

Internet: www.ProtectMaster.de
eMail: Kontakt@ProtectMaster.de

Systempartner:

TwinLock Protect Master Anleitung			
Autor:	JPS/ KTS	Info & Feedback:	Doku@ProtectMaster.de

Inhaltsverzeichnis

TwinLock ProtectMaster Einleitung

Wir freuen uns über Ihre Entscheidung, das Hochsicherheitsschloss TwinLock ProtectMaster einzusetzen. Diese Dokumentation enthält Informationen zur Konfiguration des VdS zertifizierten Hochsicherheitsschlosssystems TwinLock ProtectMaster IP 7220 und 7260.

Das Handbuch beschreibt die Konfiguration für die Systemvarianten der VdS- Klasse 2 (ProtectMaster 7260) und der VdS-Klasse 3 (ProtectMaster 7220) und bietet Informationen zu den Einstellungen.

Für weitere Informationen lesen Sie bitte auch online unter www.ProtectMaster.de oder sprechen Sie Ihren Vertiebsmitarbeiter an. Bei Anregungen und Verbesserungsvorschlägen zu dieser Anleitung oder zum Funktionsumfang, sowie der Bedienung des Systems freuen wir uns über Ihre Rückmeldung unter Doku@ProtectMaster.de.

ProtectMaster © Urheberrechtshinweis

Zertifizierungen nach DIN EN 1300, VdS-Zertifizierungen

Das TwinLock ProtectMaster System ist für alle Sicherheitsstufen zertifiziert.

Einbruch Widerstandsgrad	Anzahl Sperrpunkt (Schloss-Riegel)	Schloss Klasse gemäß ENV 1300	VdS Klasse	ProtectMaster Typ
III	1 Schloss-Riegel	Klasse B	VdS Klasse 2	7260 1-Schloss
IV	2 Schloss-Riegel	Klasse B	VdS Klasse 2	7260 2-Schloss
V	2 Schloss-Riegel	Klasse B	VdS Klasse 2	7260 2-Schloss
VI	2 Schloss-Riegel	Klasse C	VdS Klasse 3	7220 2-Schloss
VII	2 Schloss-Riegel	Klasse C	VdS Klasse 3	7220 2-Schloss
VIII	2 Schloss-Riegel	Klasse C	VdS Klasse 3	7220 2-Schloss
IX	2 Schloss-Riegel	Klasse C	VdS Klasse 3	7220 2-Schloss
X	2 Schloss-Riegel	Klasse C	VdS Klasse 3	7220 2-Schloss

1. Installation und Inbetriebnahme der Online-Netzwerkfunktionen

Das TwinLock ProtectMaster Schloss kann im Online-Modus direkt über das Netzwerk betrieben werden. Eine Netzwerkerweiterung (TwinIP) muss für den Online-Betrieb im Schloss verbaut und an das Netzwerk angeschlossen sein. Für das Einbinden des Schlosses in das Netzwerk folgen Sie der Anleitung ab Schritt xx. Alle vorherigen Schritte gehören zur mechanischen Installation und Verkabelung des Schloss-Systems.

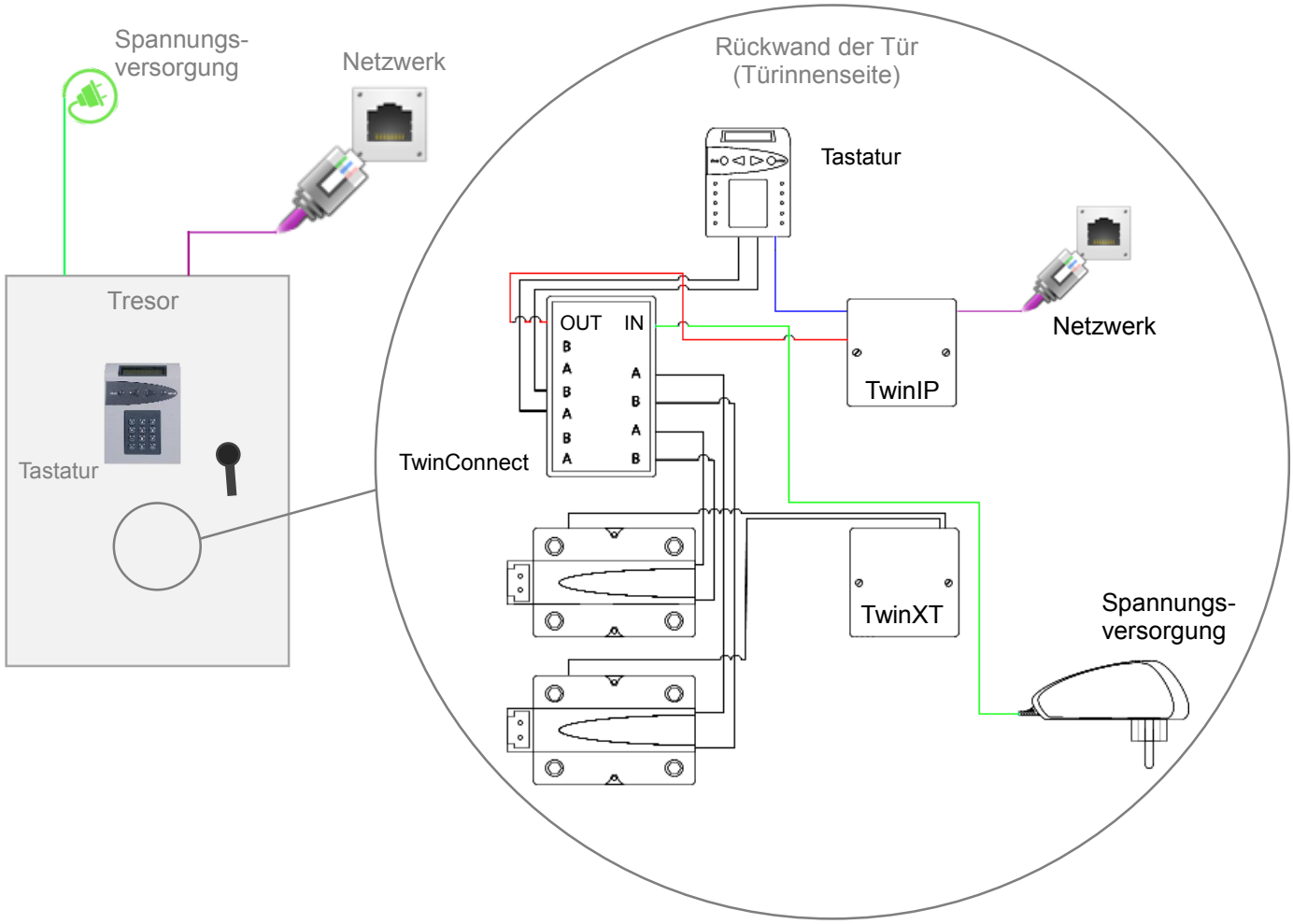
Das System TwinLock ProtectMaster ist auch ohne IP-Erweiterung voll funktionsfähig. Mit der TwinIP Erweiterung sind zusätzliche Schloss-Funktionen (Konfiguration und Administration) direkt über das Netzwerk zentral zugänglich.

2. IP-Erweiterung (TwinIP) mechanisch befestigen

Die beiden Einheiten TwinXT und TwinIP haben die gleichen Außenmaße und werden auf die gleiche Art und Weise befestigt. Bitte gehen Sie bei der Befestigung so vor, wie Sie es von der TwinXT Erweiterung kennen. Die Montage können Sie auch dem Abschnitt „Erweiterungseinheit TwinXT befestigen“ im **TwinLock Montage-Handbuch** nachlesen.

3. IP-Erweiterung (TwinIP) verkabeln und anschließen

Das folgende Schaubild zeigt die Verkabelung der Netzwerkeinheit, bzw. IP-Erweiterung (TwinIP).



4. System stromlos machen

Um die IP-Erweiterung TwinIP zu installieren, muss das System stromlos sein. Trennen Sie bitte das gesamte System von der **Spannungsversorgung**. Wenn das Schloss nicht über ein Steckernetzteil, sondern beispielsweise über den Automaten bestromt wird, entfernen Sie bitte die Spannungsversorgung am DC 12V-Eingang (IN) an der Schraubklemme der TwinConnect.

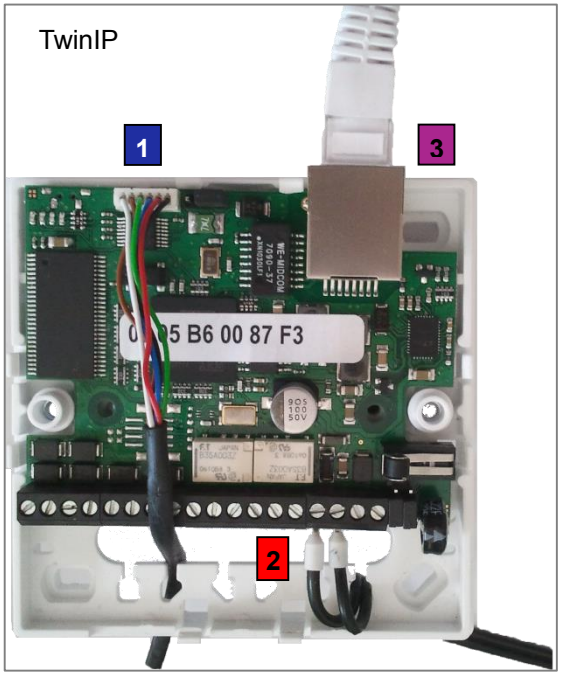
5. Deckel von TwinIP entfernen und Kabel in TwinIP einführen

Entfernen Sie den Deckel von der TwinIP, indem Sie die Befestigungsschrauben lösen. Führen Sie alle Kabel (**Netzwerk**, **Verbindung zur Tastatur** und **Spannungsversorgung**) durch den Gehäuseboden von TwinIP. Fixieren Sie die Kabel in TwinIP mit Kabelbindern und sorgen Sie so für mechanische Zugentlastung.

6. Kabelführung und Kabelanschluss

Entnehmen Sie die genaue Lage der Buchsen und Schraubklemmen bitte der Beschreibung auf der Deckelrückseite der TwinIP.

- Führen Sie das Kabel von der Tastatur-Eingabeeinheit (FlatControl) zur TwinIP (**BLAU**).
- Die 12V-Spannungsversorgung erfolgt über die TwinConnect (separater 12V Ausgang/Out) (**ROT**). An der TwinIP kommt die Spannungsversorung an Schraubklemme 3 (GND) und 4 (+12V).
- Das Netzwerkkabel (**LILA**), welches aus dem Tresor rauslegt werden muss, bzw. welches von draußen von der Netzwerkdose kommt, wird in die LAN Buchse gesteckt. Schließen Sie zuvor den Deckel der TwinIP. Benutzen Sie ein flexibles CAT 5 Netzwerkkabel.



Nr	Beschreibung
1	Anschlusskabel zur Flatcontrol (Tastatur)
2	Spannungsversorgung (3=GND und 4=+12V)
3	CAT5/ RJ45 Netzwerkanschluss

7. Anschluss und Verkabelung der TwinIP prüfen

Bestromen Sie das System, um die richtige Verkabelung zu prüfen und um die Netzwerk-Funktion zu aktivieren. Warten Sie nach dem Bestromen 2 Minuten, damit die TwinIP gestartet ist. Ab der Schloss Software-Version IP09 (Flatcontrol: Status / Info) können Sie die Netzwerk-Funktion und die IP-Adressdaten im Menü der Flatcontrol einstellen. Schalten Sie das Schloss an und drücken Sie dann mehrfach die clear-Taste. Drücken Sie anschließend 5 Sek. „enter“ (es „piept“ einmal). Gehen Sie im Menü auf „Netzwerk“, geben Sie den Systemcode ein (111111) und stellen Sie die Funktion auf „JA“. Wählen Sie bei Konfiguration „Nein“.

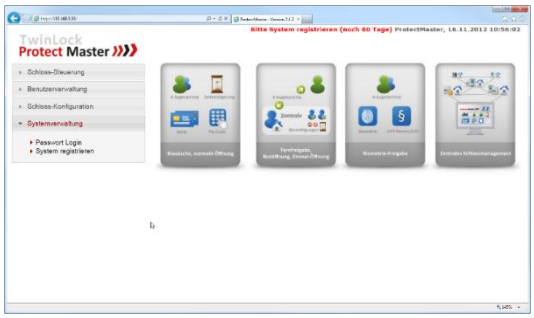
Ihnen sollte nun die Standard-IP-Adresse des Schloss-Systems angezeigt werden. Wenn Sie eine Fehlermeldung erhalten (Serial ERR oder ## 160 ##), dann folgen Sie der Anleitung ab Schritt 9.

8. Laptop verbinden und Netzwerkkabel, sowie Applikation prüfen

8.1. Verbinden Sie das Netzwerkkabel mit Ihrem PC/Laptop. Deaktivieren Sie Ihr WLAN und stellen Sie die IP-Adresse Ihres LAN-Adapters auf die folgenden Werte ein und greifen Sie anschließend per Webbrowser auf die IP-Adresse des Schlosses zu.

Ihr PC/Laptop:		**Schloss-System:**	
IP-Adresse:	**192.168.1.2**	IP-Adresse:	**192.168.1.231** oder 192.168.1.1
Subnet:	**255.255.255.0**	Subnet:	**255.255.255.0**
Gateway:	leer lassen	Gateway:	leer lassen
DNS:	leer lassen	DNS:	leer lassen

8.2. Sie sollten nun die ProtectMaster Übersichtsseite sehen. Wenn Sie die folgende Seite sehen, sind die Verkabelung und der Anschluss der IP-Erweiterung TwinIP erfolgreich. Folgen Sie der Anleitung ab Schritt 13, um das Schloss-System in das Banknetzwerk zu integrieren. Wenn Sie die Übersichtsseite nicht sehen, dann fahren Sie bitte mit Schritt 10 fort.

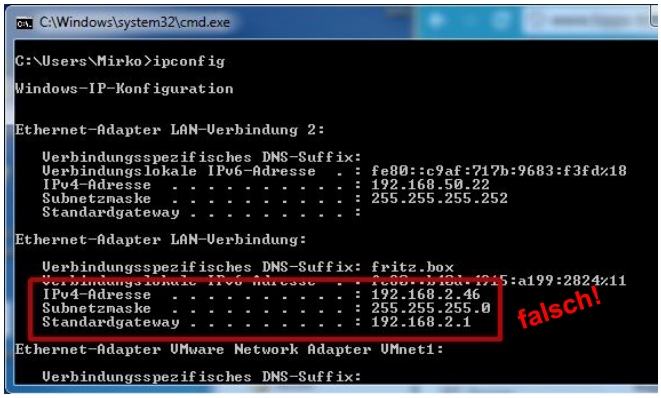


9. Fehlerdiagnose: Flatcontrol meldet: Serial ERR oder ## 160

Prüfen Sie die Kabelverbindung zwischen der Tastatur und der TwinIP (**BLAU**), tauschen Sie ggf. das Kabel. Prüfen Sie, ob die TwinIP mit ausreichend Spannung versorgt wird (12V). Die Spannungsversorgung (**ROT**) der TwinIP erfolgt über den 12V-Ausgang (OUT) der TwinConnect. Machen Sie das gesamte System einmal stromlos (Reset). Warten Sie anschließend mindestens 2 Min., um Eingaben auf der Tastatur des Schlosses zu tätigen. Führen Sie ein Reset der Tastatur (Flatcontrol) durch. Schalten Sie das Schloss an und gehen Sie im geöffneten Zustand im Menü auf „Service“ ›› „Reset“ (Achtung, nur für versierte Anwender) und folgen Sie anschließend den Schritten der normalen Schloss Inbetriebnahme (Achtung: Terminal-Wechsel anwählen!).

10. Fehlerdiagnose: IP-Adresse Ihres Laptops überprüfen (Ihre „eigene“ IP-Adresse prüfen)

Starten Sie eine Eingabe-Aufforderung auf Ihrem Laptop/PC. Klicken Sie nacheinander auf Start ›› Programme ›› Zubehör und dann auf Eingabeaufforderung oder wählen Sie alternativ Start ›› Ausführen ›› und geben Sie [cmd] (ohne eckige Klammern) ein oder drücken Sie die Windows-Taste+R und geben Sie [cmd] (ohne eckige Klammern) ein. In allen drei Varianten öffnet sich ein schwarzes Fenster. Geben Sie im Fenster [ipconfig] (ohne eckige Klammern) ein. Es erscheint folgende Anzeige:



Richtig: Ihr Ethernet-Adapter der LAN-Verbindung (nicht drahtlos) muss die unter Schritt 12 beschriebenen Daten anzeigen!

Wechseln Sie in Ihre Systemeinstellungen, Netzwerkgeräte, LAN-Adapter, Eigenschaften und gehen Sie in die Einstellungen der TCP/IP-4 Verbindung. Deaktivieren Sie WLAN und TCP/IP-6.

11. Fehlerdiagnose: Fehlerhaftes Netzwerkkabel ausschließen

Fahren Sie bitte nur fort, wenn Ihre IP-Adresse wie in Schritt 8 beschrieben und in Schritt 10 überprüft, so aussieht: **192.168.1.2.**

Gehen Sie in Ihre Netzwerkeinstellungen und prüfen Sie, ob das Netzwerkkabel zwischen Ihrem Laptop/PC und der TwinIP korrekt steckt. Das Symbol Ihrer LAN Verbindung darf nicht „Netzwerkkabel entfernt“ melden und sollte so, wie rechts dargestellt aussehen:

Wenn Sie die Kabelverbindung überprüft haben und dennoch die Meldung „Netzwerkkabel entfernt“ (links dargestellt) erscheint, dann ist vermutlich das Netzwerkkabel (**LILA**), welches aus dem Tresor herauslegt wurde, defekt. Verwenden Sie bitte zur Prüfung ein neues (normales / kein Crossover) Netzwerkkabel und verbinden Sie dies direkt mit der TwinIP und Ihrem Laptop/PC.

Wenn die Verkabelung des Systems korrekt ist und Sie die IP-Adresse Ihres Systems – wie in Schritt 12 beschrieben, korrekt eingestellt und wie in Schritt 15 beschrieben, überprüft haben, dann muss der Zugriff auf das Schloss-System funktionieren.

Bitte öffnen Sie sich erneut eine Eingabeaufforderung und geben Sie im Fenster folgendes ein: [ping 192.168.1.231] (ohne eckige Klammern). Wenn Sie Meldungen, wie z.B. „Zielsystem nicht erreichbar“, „Zeitüberschreitung“ oder „Zielhost nicht erreichbar“ erhalten, dann versuchen Sie bitte diesen Befehl: [ping 192.168.1.1] (ohne eckige Klammern).

Sie sollten bei einer der Adressen eine Antwort erhalten:

```
C:\Users\KT>ping 192.168.1.1

Ping wird ausgeführt für 192.168.1.1 mit 32 Bytes Daten:
Antwort von 192.168.1.1: Bytes=32 Zeit=2ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=255
Antwort von 192.168.1.1: Bytes=32 Zeit=1ms TTL=255

Ping-Statistik für 192.168.1.1:
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0
    (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 2ms, Mittelwert = 1ms
```

Wenn Sie keine Antwort erhalten, überprüfen Sie nochmals alle Schritte dieser Anleitung oder kontaktieren Sie unseren Service.

Sofern Sie eine Antwort erhalten, jedoch nicht wie in Schritt 8.2 beschrieben, eine ProtectMaster Übersichtsseite im Webbrowser sehen, folgen Sie bitte der Anleitung in Schritt 14.

12. Zugriff auf das Webinterface

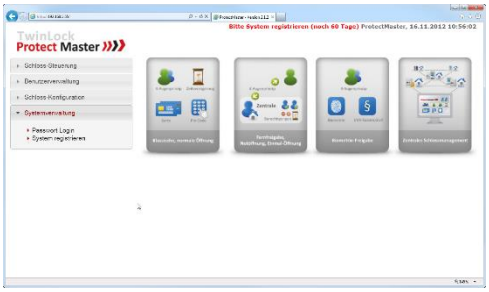
Verwenden Sie bitte einen alternativen Webbrowser (z.B. Firefox) und stellen Sie sicher, dass Sie **keinen** Proxy hinterlegt haben.

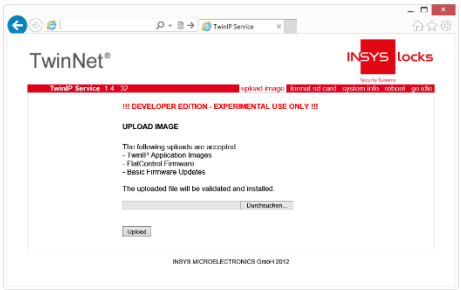
- **Internet-Explorer**: Internetoptionen ›› Verbindungen ›› LAN Einstellungen ›› Proxy (muss deaktiviert sein)
- **Fire-Fox**: Einstellungen ›› Einstellungen ›› Verbindungen ›› Erweitert ›› Netzwerk ›› Einstellungen ›› Proxy ›› kein Proxy.

Schließen Sie alle Browserfenster und starten Sie Ihren Browser neu. Versuchen Sie sich erneut die folgenden Adressen aufzurufen:

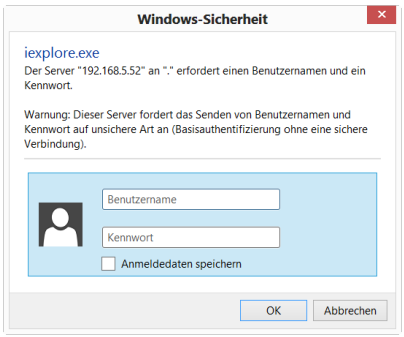
- http://192.168.1.1 oder http://192.168.1.1:8080 (Passwort Abfrage)
- http://192.168.1.231 oder http://192.168.1.231:8080 (Passwort Abfrage)

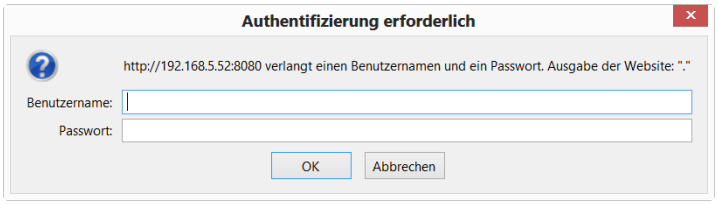
Sie sollten bei einer der Adressen anstelle einer Fehlerseite (404 – Internetseite nicht verfügbar) die folgenden Seiten sehen:





Oder Sie erhalten eine Passwort-Abfrage:





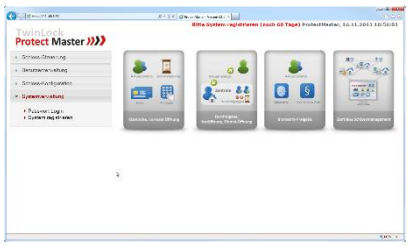
Wenn Sie eine der genannten Seiten sehen oder eine Passwortabfrage erhalten, ist die Verkabelung und Installation **erfolgreich** abgeschlossen. Ihr System benötigt lediglich eine Software-Aktualisierung. Folgen Sie dem Schritt 14 (TwinNet Oberfläche oder Passwort Abfrage), um die Software zu aktualisieren.

13. Netzwerkeinstellungen des Schlosses auf die vorgegeben Bank-Adress-Daten ändern

Bei korrekter Installation und Verkabelung des Schloss-Systems können Sie die IP-Adresse des Schlosses auf zwei unterschiedliche Arten ändern (über das Webinterface oder über die Tastatur des Schlosses).

13.1. **IP-Adresse des Schlosses über die Weboberfläche konfigurieren:**

Die ProtectMaster Oberfläche erreichen Sie, indem Sie im Webbrowser folgende Adresse eingeben: 192.168.1.231 – Ihr Laptop/PC muss hierfür auf dem in Schritt 12 beschriebenen Adressbereich stehen. Sie sollten folgende Übersichtsseite sehen:



Wenn Sie diese Seite nicht sehen, folgen Sie bitte den Anweisungen im Schritt 15.

Klicken Sie auf den Menüpunkt ► Systemverwaltung ► Login geben Sie bitte als ID „**10012**“ und als Passwort „**safecor2005**“ ein.

Klicken Sie auf den Menüpunkt ► Systemverwaltung ► Netzwerk einstellen. Geben Sie bitte die Netzwerkdaten ein, welche Sie vom Verantwortlichen Bank-Administrator zu Verfügung gestellt bekommen haben. Bei automatischen DHCP-Adressdaten vergewissern Sie sich bitte, ob jene Daten korrekt sind, da Sie andernfalls nach erfolgter Umstellung das Gerät nicht wieder erreichen können. Es ist daher immer ratsam das ProtectMaster Schloss zunächt über eine feste IP-Adresse in Betrieb zu nehmen und anschließend ggf. auf das automatische DHCP Verfahren umzustellen.

13.2. **IP-Adresse des Schlosses über die Schloss-Tastatur konfigurieren:**

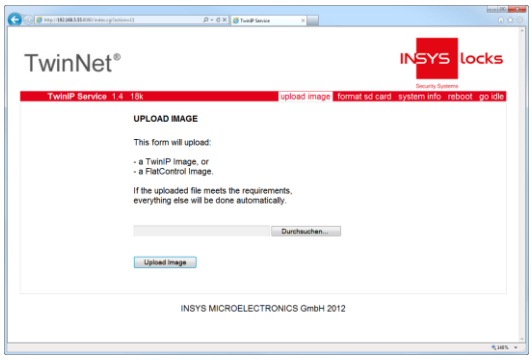
Ab der Schloss Software-Version IP09 (Flatcontrol: Status / Info) können Sie die Netzwerk-Funktion und die IP-Adressdaten im Menü der Flatcontrol einstellen.
► Schalten Sie das Schloss an und drücken Sie dann mehrfach die clear-Taste.
► Drücken Sie anschließend 5 Sek. „enter“ (es „piept“ einmal).
► Gehen Sie im Menü auf „Netzwerk“, geben Sie den Systemcode ein (111111)
► Stellen Sie die Funktion auf „JA“ und wählen Sie bei Konfiguration „JA“.

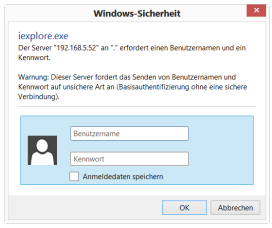
Wenn Sie anschließend eine Fehlermeldung erhalten (Serial ERR oder ## 160 ##), machen Sie das System bitte einmal vollständig stromlos und warten Sie nach dem Bestromen ca. 2 Min. bevor Sie sich den Menüpunkt erneut aufrufen.

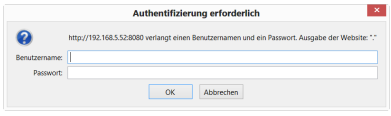
Sie können nun die IP-Adressdaten (feste IP-Adresse oder DHCP) eingeben. Alle Eingaben erfolgen immer dreistellig (010.006.123.001 anstelle von 10.6.123.1). Bitte hinterlegen Sie keine DNS-Adresse und bestätigen Sie die Abfrage der DNS-Adresse mit enter.

14. Bei Aufruf der Webseite erscheint die „TwinNet“ Übersichtsseite oder es erscheint eine User/ Passwort Abfrage.

Beim Aufruf der Weboberfläche erscheint eine TwinNet (Insys locks) Übersichtsseite oder eine Passwort-Abfrage und nicht die ProtectMaster Oberfläche:







Bitte laden Sie sich die aktuelle ProtectMaster Software Version aus dem Safecor WebPortal herunter und folgen Sie den Anweisungen für die Aktualisierung der ProtectMaster Software.

Es gibt zwei Möglichkeiten die Aktualisierung durchzuführen.

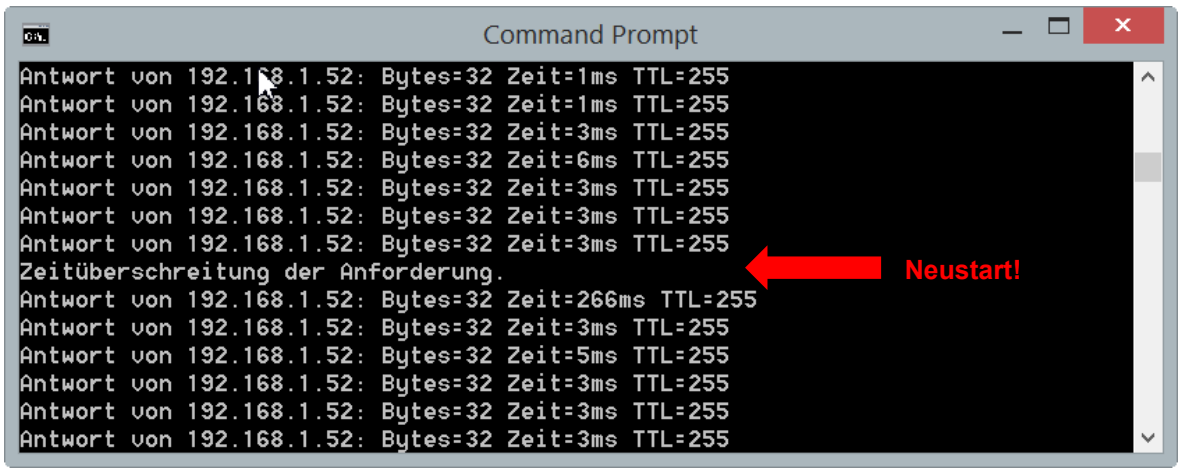
15. Aktualisierung der ProtectMaster Software (Update der Version) mit Toolbox

Gehen Sie bitte wie folgt vor, um die aktuellste ProtectMaster Version aufzuspielen:

Laden Sie sich bitte die aus dem Portal http://update.protectmaster.de die aktuelle Toolbox herunter. Laden Sie sich zusätzlich das aktuelle PortectMaster Image (Toolbox) herunter. Die Login-Daten für das Portal erhalten Sie von Ihrem zuständigen Vertriebsmitarbeiter oder dem technischen Support.

Bitte gehen Sie exakt nach Reinfolge vor:

0. Bitte starten Sie sich eine Eingabeaufforderung [cmd] und setzen Sie einen Dauer-Ping auf das Schloss, um den Neustart bei Updateprozess zu überprüfen.
   Beispiel: [ping 192.168.1.1 –t]



1. Bitte starten Sie das ProtectMaster Schloss neu. Gehen Sie in die Weboberfläche (im Browser) unter ► Systemverwaltung ► Passwort Login und anschließend ► Systemverwaltung ► System neu starten. Alternativ trennen Sie das Schloss-System bitte einmal von der Spannungsversorgung. Warten Sie nach dem Neustart min. 3 Min.

2. Entpacken Sie bitte beide heruntergeladene ZIP-Dateien. Starten Sie im entpackten Verzeichnis die Toolbox2.

3. Gehen Sie bitte im gestarteten Toolbox-Programm auf ›› Datei ›› neues Gerät hinzufügen und wählen Sie PROTECTMASTER und die IP-ADRESSE des Schlosses.

4. Gehen Sie im Toolbox-Programm auf ›› Update ›› Update Datei einlesen und wählen sie im entpackten ProtectMaster-Update Ordner die Datei „ProtectMaster_2.*x.x*.bin“.

5. Wählen Sie im Toolbox-Programm in der linken Liste das Schloss aus und gehen Sie rechts auf Update ohne Neustart.

6. Das Update wird nun übertragen. Nach ca. 5 Min. können Sie sich die neue ProtectMaster Version in der Browseroberfläche aufrufen.

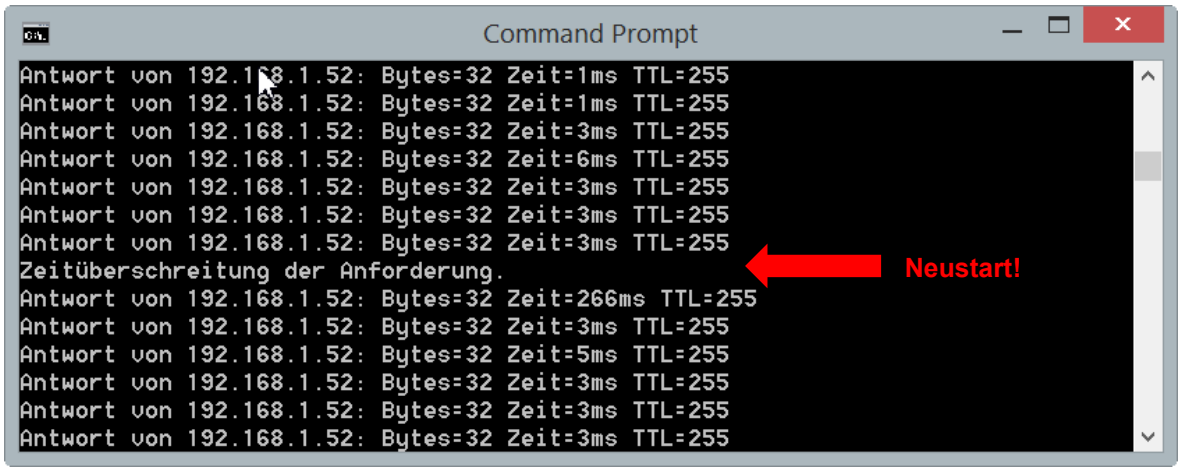
Sie haben Ihr ProtectMaster Schloss erfolgreich installiert und können es im Webbrowser aufrufen.

16. Aktualisierung der ProtectMaster Software (Update der Version) über Webinterface

Laden Sie sich bitte die aus dem Portal http://update.protectmaster.de das aktuelle PortectMaster Image (Web) herunter. Die Login-Daten für das Portal erhalten Sie von Ihrem zuständigen Vertriebsmitarbeiter oder dem technischen Support.

Bitte gehen Sie exakt nach Reinfolge vor:

7. Bitte starten Sie sich eine Eingabeaufforderung [cmd] und setzen Sie einen Dauer-Ping auf das Schloss, um den Neustart bei Updateprozess zu überprüfen.
   Beispiel: [ping 192.168.1.1 –t]



8. Bitte starten Sie das ProtectMaster Schloss neu. Gehen Sie in die Weboberfläche (im Browser) unter ► Systemverwaltung ► Passwort Login und anschließend ► Systemverwaltung ► System neu starten. Alternativ trennen Sie das Schloss-System bitte einmal von der Spannungsversorgung. Warten Sie nach dem Neustart min. 3 Min.

9. Entpacken Sie bitte die heruntergeladene ZIP-Datei.

10. Rufen Sie sich die IP-Adresse des Schlosses auf und geben Sie hinter der IP-Adresse [:8080] (ohne die eckigen Klammern) ein. Beispiel: http://192.168.1.1:8080

11. Im Passwortfenster geben Sie als Usernamen [**twinip**] und als Passwort [**hifoko64**] ein.

12. Gehen Sie im Menü auf ► „upload image“ ► Durchsuchen und wählen Sie die entpackte AES-Datei aus. Klicken Sie auf ► Upload und warten Sie min. 5 Min.

13. Es erscheint „Done“ und das System startet selbständig neu.

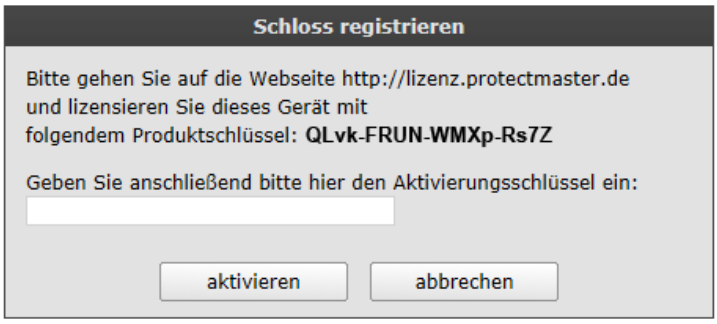
Sie haben Ihr ProtectMaster Schloss erfolgreich installiert und können es im Webbrowser aufrufen.

17. System registrieren

Sie müssen Ihr Schloss-System bitte registrieren, um die Einrichtung des Schloss-System erfolgreich abzuschließen. Ihr System ist noch nicht vollständig eingerichtet, wenn Sie das Schloss im Webbrowser aufrufen und oben rechts in der Ecke folgende Meldung erscheint:

nicht registriertes System (noch 60 Tage) , 22.05.2011 10:36:31

Bitte rufen Sie sich das Menü ► **Systemverwaltung** ► **System registrieren** auf.



Markieren und kopieren Sie sich den angezeigten Produktschlüssel (*in diesem Beispiel: QLvk-FRUN-WMXp-Rs7Z*). Bitte achten Sie darauf, vor und nach dem Produktschlüssel keine Leerzeichen zu kopieren. Öffnen Sie sich ein neues Browserfenster und wechseln Sie auf die Webseite http://lizenz.protectmaster.de.

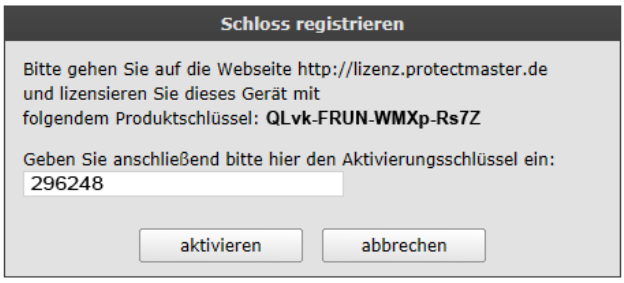
Füllen Sie das Formular aus. Sie erhalten nach wenigen Minuten den Aktivierungsschlüssel an Ihre E-Mail Adresse geschickt.

Beispiel des E-Mail Textes:
Vielen Dank für die Registrierung Ihres ProtectMaster Netzwerk-Tresorschlosses. Der Lizenzschlüssel für dieses Schloss lautet: 296248

Markieren und kopieren Sie sich den angezeigten Lizenzschlüssel (*in diesem Beispiel:296248*). Bitte achten Sie darauf, vor und nach dem Schlüssel keine Leerzeichen zu kopieren.

Bitte geben Sie den Lizenzschlüssel in der Weboberfläche des Schlosses im Menü unter ► **Systemverwaltung** ► **System registrieren** ein.

Beispiel:



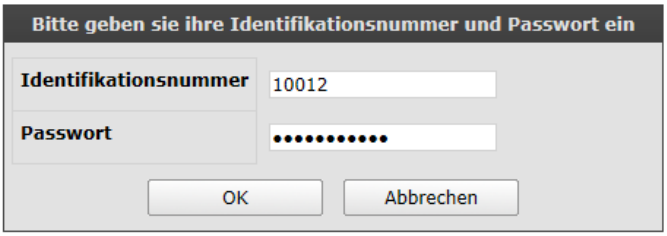
Schließen Sie den Vorgang mit ► **aktivieren** ab.

Die rote Registrierungs-Meldung in der oberen rechten Ecke sollte jetzt verschwunden sein.

18. Erstanmeldung: Am System als WEB-Administrator anmelden

Bitte rufen Sie sich das Menü ► **Systemverwaltung** ► **Passwort Login** auf.

Für die erste Anmeldung am System verwenden Sie bitte die folgenden Anmeldedaten:
Identifikationsnummer: **10012**
Passwort: **safecor2005**

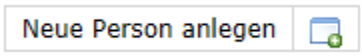


Sie sind jetzt am System angemeldet und können unter dem Menü-Punkt Konfiguration Geräte verwalten und Stammdaten editieren.

19. Einen WEB-Administrator anlegen/ einrichten

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Benutzerverwaltung** ► **Benutzermatrix** auf.

Wählen Sie den Punkt ► **neue Person anlegen**.



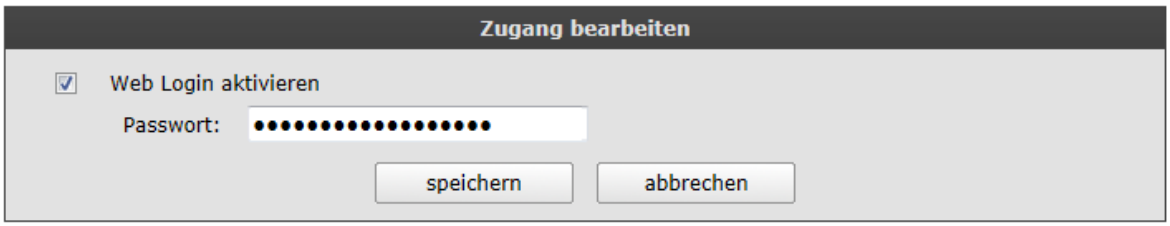
Hinterlegen Sie die gewünschten Daten für den WEB-Administrator:

- **Anrede**: frei wählbar (z.B. Frau, Herr, Gruppe, Systemuser, etc.)
- **Vorname**: frei wählbar (z.B. Max)
- **Nachname**: frei wählbar (z.B. Mustermann)
- **ID.Nr**: Personalnummer (bitte hinterlegen Sie eine zwei- bis sechsstellige Zahl)
- **Schloss UserID**: Vergeben Sie dem Web-Admin keinen Schloss UserID.

Schließen Sie den Dialog mit ► **speichern** ab.

Der angelegte Benutzer taucht nur in der Stammdatenübersicht auf. Wählen Sie bitte in der Zeile des neu angelegten Benutzers das Symbol „Berechtigungen zuweisen“.

Zeile des Benutzers auswählen und den Button [ ] ► **Berechtigungen zuweisen** anwählen. ► **aktivieren** Sie den **Web Login** und vergeben Sie ein Start-Passwort. Der Benutzer kann dieses zu einem späteren Zeitpunkt ändern.



Vergeben Sie abschließend die Rechte für den WEB Administrator, indem Sie in der 1. Spalte Web-Master aus dem [✗] einen Haken [✔] machen. ► klicken Sie hierzu auf das Symbol [✗].

Der neu angelegte User, welcher WEB-Administrator werden soll, hat nun ein Passwort vergeben bekommen und in der Spalte WEB-Master die entsprechenden Rechte.

Bevor Sie bestehende WEB-Administratoren löschen oder deren Rechte verändern, melden Sie sich zunächst ab und mit den neu angelegten Benutzerdaten erneut an, um diese zu testen.

. ► **Systemverwaltung** ► **Logout**.
. ► **Systemverwaltung** ► **Passwort Login**.

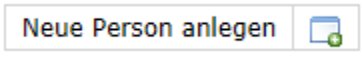
Melden Sie sich nun mit der Identifikationsnummer und dem Passwort des neu angelegten Benutzers an. Unter dem Menü ► **Konfiguration** ► **Benutzerverwaltung** sollten Sie nun die Möglichkeit haben, neue Personen anzulegen.

Sie können nun den Web-Master für die Erstanmeldung (ID: 10012) ändern/löschen.

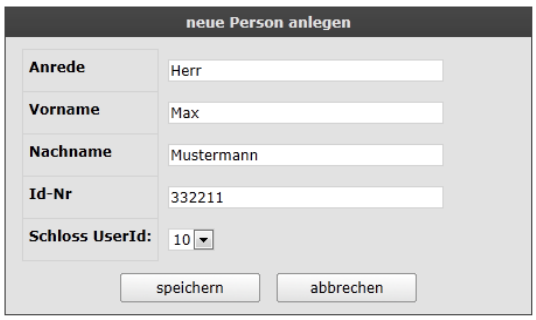
20. Einen neuen Schloss-Benutzer anlegen/ einrichten

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Konfiguration** ► **Benutzerverwaltung** auf.

Wählen Sie den Punkt ► **neue Person anlegen**.



Hinterlegen Sie die gewünschten Daten für den neuen Benutzer:



- **Anrede**: frei wählbar (z.B. Frau, Herr, Gruppe, Systemuser, etc.)
- **Vorname**: frei wählbar (z.B. Max)
- **Nachname**: frei wählbar (z.B. Mustermann)
- **Id.Nr**: frei wählbar (bitte hinterlegen Sie eine ein- bis sechsstellige Zahl)
- **Schloss UserID**: die Benutzernummer am Schloss (es werden nur die freien Benutzernummern vorgeblendet)

Schließen Sie den Dialog mit ► **speichern** ab.

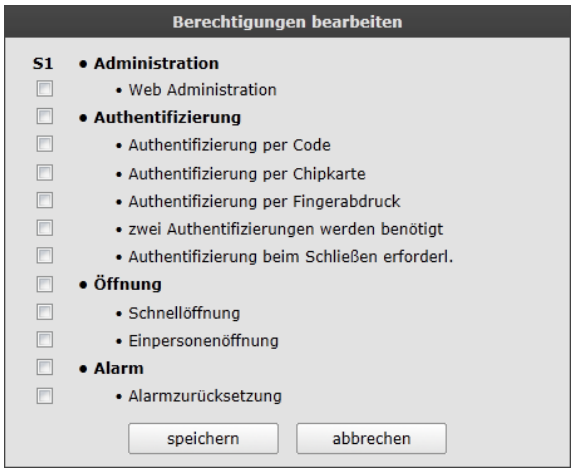
Der angelegte Benutzer taucht nun in der Stammdatenübersicht auf. Wählen Sie bitte in der Zeile des neu angelegten Benutzers das Symbol „**Berechtigung bearbeiten**“.

Zeile des Benutzers auswählen und den Button [ ] ► **Berechtigung bearbeiten** anwählen.
► **aktivieren** Sie die gewünschten **Rechte** gemäß nachfolgender Beschreibung.

Im Standardfall soll der Benutzer beispielsweise mit einem persönlichen PIN-Code das Schloss öffnen. Aktivieren Sie entsprechend „**Authentifizierung per Code**“.

Wenn der Benutzer das Schloss mit einer Chipkarte und ohne Code öffnen soll, aktivieren Sie bitte „**Authentifizierung per Chipkarte**“.

Wenn der Benutzer das Schloss mit einer Chipkarte und mit einem Code öffnen soll, aktivieren Sie bitte „**Authentifizierung per Chipkarte**“, „**Authentifizierung per Code**“, sowie die Einstellung „**zwei Authentifizierungen werden benötigt**“. Der Benutzer muss in diesem Fall sowohl die Chipkarte, als auch einen Code eingeben, um Öffnen zu können.



Erläuterung:

Bezeichnung	Funktion
Web Administration	Darf das Schloss über den Web-Zugriff verwalten, User anlegen, etc.
Authentifizierung per Code	Benutzer muss sich mit einem PIN-Code am Schloss authentifizieren, um es öffnen zu können. → *Benutzernummer + PIN-Code*
Authentifizierung per Chipkarte	Benutzer muss sich mit einer Chipkarte am Schloss authentifizieren, um es öffnen zu können. → *Benutzernummer + Chipkarte*
Authentifizierung per Fingerabdruck	Benutzer muss, um sich am Schloss per Code oder Chipkarte authentifizieren zu können, zuvor biometrisch authentifizieren. Diese Einstellung ist für den UVV-Kassen konformen Betrieb in Kleinstzweigstellen erforderlich. → *biometrische Freigabe über Fingerprint-System gefolgt von Benutzernummer + PIN-Code oder Chipkarte*
zwei Authentifizierungen werden benötigt	Wenn diese Funktion, sowie Code und Chipkarte als Authentifizierungsart aktiviert sind, muss der Benutzer sich mit PIN-Code und Chipkarte am Schloss authentifizieren, um es öffnen zu können. → *Benutzer-nummer + Chipkarte + PIN-Code*
Authentifizierung beim Schließen erforderlich	Wenn “Global” für das Schloss-System konfiguriert wurde, dass zum Schließen des Schlosses eine Authentifizierung erforderlich ist, so dürfen diese Benutzer das Schloss schließen. Benutzer, welche diese Berechtigung nicht erhalten, dürfen nicht schließen.
Schnellöffnung	Wenn “Global” für das Schloss-System eine Zeitverzögerung für das Öffnen konfiguriert wurde, dann sind diese Benutzer berechtigt, jene Zeitverzögerung zu umgehen. Benutzer, welche diese Berechtigung nicht erhalten, müssen die Zeitverzögerung abwarten.
Einpersonenöffnung	Wenn “Global” für das Schloss-System eine 4-Augen Öffnung konfiguriert wurde, dann sind diese Benutzer berechtigt, jenes 4-Augen-Prinzip zu umgehen. Benutzer, welche diese Berechtigung nicht erhalten, müssen im 4-Augen-Prinzip öffnen. Diese Einstellung greift aktuell nur bei 1-Schloss-Systemen.
Alarmzurücksetzung	Wenn über das Schloss-System eine EMA „scharf“ oder „unscharf“ geschaltet wird, dann sind diese Benutzer berechtigt, den Alarm „unscharf“ zu schalten. Benutzer, welche diese Berechtigung nicht erhalten, können das Schloss nicht „unscharf“ schalten.

Vergeben Sie die gewünschten Rechte und schließen Sie den Dialog mit ► **speichern** ab.

In der Tabelle sollten die aktivierten Rechte entsprechend mit einem Haken [✔] versehen sein und es sollten die deaktivierten Rechte entsprechend mit einem Haken [✗] versehen sein.

Korrigieren Sie gegebenenfalls die Rechte, indem Sie erneut den Button [ ] ► **Berechtigung bearbeiten** aufrufen.

Der Benutzer hat nun die erforderlichen Rechte für das Schloss-System. Im nächsten Schritt muss nun der eigentliche persönliche PIN-Code des Benutzers oder die Chipkarte am Schloss – System angelegt werden.

21. Einen neuen PIN-Code oder eine neue Chipkarte am Schloss anlegen

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Konfiguration** ► **Benutzerverwaltung** auf.

Um einen geheimen PIN-Code oder eine Chipkarte am Schloss neu anzulegen, benötigen Sie vor Ort einen Benutzer, welcher bereits am Schloss-System mit einem PIN-Code berechtigt ist oder alternativ eine bereits am Schloss-System angelernte Chipkarte.

Überprüfen Sie, ob für den Benutzer, für welchen Sie einen Code oder eine Chipkarte anlegen wollen, über die erforderlichen Rechte verfügt (mindestens PIN Code oder Chipkarte).

Wählen Sie in der Zeile des Benutzers für welchen Sie einen Code oder eine Chipkarte neu anlegen wollen, den Button [ ] ► **Berechtigungen zuweisen**. Wählen Sie im nächsten Dialog den Benutzer vor Ort, welcher bereits über einen PIN-Code oder eine Chipkarte verfügt und klicken Sie auf den Button ► **Programmier-TAN**. Es wird Ihnen eine Anleitung vorgebeldnet.

Leiten Sie die beiden Benutzer vor Ort entsprechend der Anweisung an oder verschicken Sie alternativ die Anleitung per E-Mail, indem Sie den Text markieren, kopieren und in die E-Mail einfügen.

Sobald die Benutzer vor Ort die Programmierung nach der Anleitung durchgeführt haben, ist der PIN-Code aktiv und angelegt.

Der Code bleibt auch im Schloss gültig, wenn Sie dem Benutzer die Rechte zum Öffnen entziehen. Der Benutzer kann in diesem Fall dann nicht mehr öffnen, aber bei erneuter Aktivierung der erforderlichen Rechte wird der bereits im Schloss-System hinterlegte Code wieder aktiv und der Benutzer kann wieder öffnen. Das Entziehen der Rechte führt also nicht automatisch zum Löschen des PIN-Codes, bzw. der Chipkarte.

22. Notfall-Benutzer einrichten

Wenn Sie für bestimmte Notfälle einen besonderen Benutzer einrichten wollen, dann hat sich das folgende Konzept bewährt. Beachten Sie, dass diese Einstellungen nur greifen können, wenn Sie die Konfiguration des Notfall-Benutzers vornehmen, bevor die Notfall-Situation eintritt und nicht erst, wenn es bereits zu jener Situation kommt.

Als Notfall gilt häufig eine Situation, wo ein Benutzer allein vor Ort das Schloss-System öffnen soll, das Schloss-System aber nur für eine Öffnung im 4-Augen-Prinzip konfiguriert ist und entsprechend keine Möglichkeit für den Benutzer vor Ort besteht, das Schloss allein zu öffnen.

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Konfiguration** ► **Benutzerverwaltung** auf.

Wählen Sie den Punkt ► **neue Person anlegen**.

Hinterlegen Sie die gewünschten Daten für den neuen Notfall-Benutzer:

- **Anrede**: Gruppe
- **Vorname**: User
- **Nachname**: Notfall
- **Id.Nr**: frei wählbar
- **Schloss UserId**: die Benutzernummer am Schloss (z.B. 90)

Schließen Sie den Dialog mit ► **speichern** ab.

Je nachdem, ob Sie einen Notfall-PIN oder eine Notfall-Chipkarte nutzen wollen, aktivieren Sie die entsprechenden Berechtigungen.

Wählen Sie die Zeile des Notfall-Benutzers und den Button [ ] ► **Berechtigung bearbeiten**. ► **aktivieren** Sie „**Authentifizierung per Code**“ oder „**Authentifizierung per Chipkarte**“´und schließen Sie den Dialog mit ► **speichern** ab.

Wählen Sie in der Zeile des Notfall-Benutzers den Button [ ] ► **Berechtigungen zuweisen**. Wählen Sie im nächsten Dialog einen Benutzer vor Ort, welcher bereits über einen PIN-Code oder eine Chipkarte verfügt und klicken Sie auf den Button ► **Programmier-TAN**.

Leiten Sie den Benutzer vor Ort entsprechend der Anweisung an oder verschicken Sie alternativ die Anleitung per E-Mail, indem Sie den Text markieren, kopieren und in die E-Mail einfügen.

Wenn Sie als Authentifizierungs-Art PIN-Code und nicht Chipkarte gewählt haben, geben Sie dem Benutzer vor Ort noch einen geheimen PIN-Code vor (z.B. 123456).

Sobald der Benutzer vor Ort die Programmierung nach der Anleitung durchgeführt hat, ist der PIN-Code, bzw. die Chipkarte aktiv und angelegt.

Damit der Code oder die Karte nur im Notfall benutzt werden kann, deaktivieren Sie jetzt wieder das vergebene Recht, indem Sie auf den grünen Haken [✔] neben dem Notfall-User klicken.

Der Notfall-User sollte anschließend über keine Rechte verfügen:

Id-Nr	Benutzer	Anrede	Name	Vorname					Web-Master	PIN Code	Chipkarte	Biometrie	min. 2 aus X	Schließer	ohne Zeitverz.	2-Augen	EMA
10000	1	Gruppe	Notfall	User					✗	✗	✗	✗	✗	✗	✗	✗	✗

Wenn die Not-Situation eintritt, vergeben Sie entsprechend wieder das Recht, welches Sie dem Notfall-User zugeordnet hatten, indem Sie auf das rote Kreuz neben dem Notfall-User klicken.

Die Berechtigung wechselt von nicht vergeben (nicht aktiv) [✗] ► auf [✔] vergeben (aktiv).

Der Notfall-User ist immer nur dann aktiv, wenn Sie das entsprechende Recht vergeben haben.

Wenn Sie einen geheimen Notfall-PIN-Code nutzen, kann mit diesem Code nur dann geöffnet werden, wenn Sie das Recht für PIN Code vergeben [✔] haben. Wenn Sie das Recht entziehen [✗], ist es nicht mehr möglich, mit dem PIN-Code zu öffnen.

Wenn Sie eine Notfall-Chipkarte in der Geschäftsstelle hinterlegt haben, kann mit dieser Karte nur dann geöffnet werden, wenn Sie das Recht für Chipkarte vergeben [✔] haben. Wenn Sie das Recht entziehen [✗], ist es nicht mehr möglich, mit der Karte zu öffnen.

23. Programmier-Benutzer einrichten

Der Standard Anlern-Vorgang eines neuen Benutzers im Schloss-System erfolgt immer im 4-Augen-Prinzip. Der neue Mitarbeiter und eine bereits im Schloss-System hinterlegter Benutzer müssen den Programmier-Vorgang vor Ort abschließen, damit der neue Benutzer aktiv wird.

Wenn Sie das Vergeben von PIN-Codes oder das Anlernen von Chipkarten für den Öffnungsvorgang nicht im 4-Augen-Prinzip durchführen wollen, sondern der neue Benutzer vor Ort die Programmierung seiner Öffnungsberechtigung allein, bzw. mit Ihrer Unterstützung durchführen können soll, dann legen Sie sich bitte einen Programmier-Benutzer an.

Beachten Sie, dass diese Einstellungen nur greifen können, wenn Sie die Konfiguration des Programmier-Benutzers vornehmen, bevor Sie die erste Programmierung eines neuen Benutzers durchführen wollen und nicht erst, wenn es bereits zu jener Situation kommt.

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Konfiguration** ► **Benutzerverwaltung** auf.

Wählen Sie den Punkt ► **neue Person anlegen**.

Hinterlegen Sie die gewünschten Daten für den neuen Programmier-Benutzer:

- **Anrede**: Gruppe
- **Vorname**: User
- **Nachname**: Programmier
- **Id.Nr**: frei wählbar
- **Schloss UserId**: die Benutzernummer am Schloss (z.B. 91)

Schließen Sie den Dialog mit ► **speichern** ab.

Wählen Sie die Zeile des Programmier-Benutzers und den Button [ ] ► **Berechtigung bearbeiten** und ► **aktivieren** Sie „**Authentifizierung per Code**“ und schließen Sie den Dialog mit ► **speichern** ab.

Wählen Sie in der Zeile des Programmier-Benutzers den Button [ ] ► **Berechtigungen zuweisen**. Wählen Sie im nächsten Dialog einen Benutzer vor Ort, welcher bereits über einen PIN-Code verfügt und klicken Sie auf den Button ► **Programmier-TAN**.

Leiten Sie den Benutzer vor Ort entsprechend der Anweisung an oder verschicken Sie alternativ die Anleitung per E-Mail, indem Sie den Text markieren, kopieren und in die E-Mail einfügen.

Geben Sie dem Benutzer vor Ort noch abschließend einen geheimen PIN-Code vor (z.B. 123456).

Sobald der Benutzer vor Ort die Programmierung nach der Anleitung durchgeführt hat, ist der PIN-Code aktiv und angelegt.

Damit der Code nur die Programmierung neuer Benutzer benutzt werden kann, deaktivieren Sie jetzt wieder das vergebene Recht, indem Sie auf den grünen Haken [✔] neben dem Programmier-User klicken.

Der Programmier-User sollte anschließend über keine Rechte verfügen:

Id-Nr	Benutzer	Anrede	Name	Vorname					Web-Master	PIN Code	Chipkarte	Biometrie	min. 2 aus X	Schließer	ohne Zeitverz.	2-Augen	EMA
10000	1	Gruppe	Programmier	User					✘	✘	✘	✘	✘	✘	✘	✘	✘

Wenn die Situation eintritt, dass ein neuer Benutzer im 2-Augen-Prinzip allein seinen eigenen PIN-Code oder seine eigene Chipkarte anlegen soll, vergeben Sie entsprechend wieder das Recht, welches Sie dem Programmier-User zugeordnet hatten, indem Sie auf das rote Kreuz neben dem User klicken.

Die Berechtigung wechselt von nicht vergeben (nicht aktiv) [✘] ► auf [✔] vergeben (aktiv).

Der Notfall-User ist immer nur dann aktiv, wenn Sie das entsprechende Recht vergeben haben.

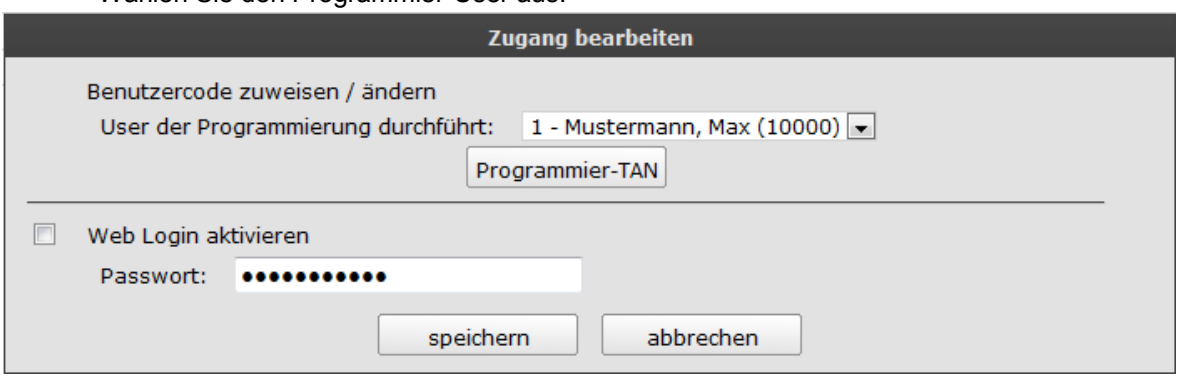
Wenn Sie einen geheimen Programmier-PIN-Code nutzen, kann mit diesem Code nur dann programmiert werden, wenn Sie das Recht für PIN Code vergeben [✔] haben. Wenn Sie das Recht entziehen [✘], ist es nicht mehr möglich, mit dem PIN-Code zu programmieren.

Wenn Sie eine Programmier -Chipkarte in der Geschäftsstelle hinterlegt haben, kann mit dieser Karte nur dann programmiert werden, wenn Sie das Recht für Chipkarte vergeben [✔] haben. Wenn Sie das Recht entziehen [✘], ist es nicht mehr möglich, mit der Karte zu programmieren.

Damit die Karte oder der PIN-Code nicht für Öffnungen missbraucht wird, deaktivieren Sie die Rechte des Programmier-Users nach jeder erfolgten Programmierung umgehend.

So gehen Sie vor, um den Programmier-User zu nutzen, bzw. einen neuen Benutzer zu programmieren:

- Aktivieren Sie die Rechte des Programmier-Users.
- Legen Sie den neuen Benutzer mit entsprechenden Rechten an.
- Rufen Sie sich die Authentifizierung [ ] des neuen Benutzers auf, für welchen Sie einen PIN-Code oder eine Chipkarte vergeben/anlernen wollen.
- Wählen Sie den Programmier-User aus:



- Klicken Sie auf den Button „Programmier-TAN“
- Folgen Sie der Anleitung und nennen Sie dem neuen Benutzer vor Ort Ihren geheimen Programmier-PIN Code oder den Ort, wo Sie Ihre Programmier-Chipkarte hinterlegt haben.
- Deaktivieren Sie die Rechte des Programmier-Users.

24. Einmal-Benutzer einrichten / Fernwirken aus einer Zentrale einrichten

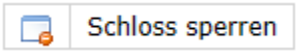
Wenn Sie die volle Kontrolle über das Öffnen eines Schloss durch einen bestimmten Benutzer haben möchten, bzw. die Öffnungen durch eine Zentralle kontrollieren lassen möchten, dann können Sie das Fernwirken aus der Zentrale auf zwei verschiedene Arten realiesieren. Für das Fernwirken gibt es verschiedene Bezeichnungen, wie z.B. Einmalöffnung, Einmalcode, flüchtiger Code, Zentral-Freigabe, PIN-TAN-Verfahren, etc.

- Variante: Kein Benutzer darf das Schloss ohne Freigabe aus der Zentrale öffnen.
- Variante: Ein bestimmter Benutzer muss sich für jeden oder eine bestimmte Anzahl von Öffnungsvorgängen des Schlosses „freischalten“ lassen.

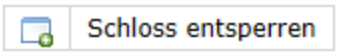
Bei der ersten Variante muss sich jeder Benutzer in der Zentrale (beim Web-Administrator) melden, um eine Schloss-Öffnung durchführen zu können. Der Web-Administrator „aktiviert“ den Öffnungsvorgang und „sperrt“ das Schloss-System anschließend wieder.

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Steuerung** ► **Schloss-Status und globales Sperren** auf.

Wählen Sie anschließend Schloss sperren, um alle Öffnungsvorgänge zu deaktivieren und wählen Sie Schloss entsperren, um den Öffnungsvorgang freizugeben.



Im gesperrten Zustand besteht für keinen Benutzer eine Möglichkeit das Schloss zu öffnen.



Im entsperrten Zustand kann jeder Berechtigte Benutzer das Schloss mit PIN-Code oder Chipkarte öffnen.

Bei der zweiten Variante muss sich ein bestimmter Benutzer in der Zentrale (beim Web-Administrator) melden, um eine oder mehrere Schloss-Öffnung(en) durchführen zu können.

Bitte melden Sie sich am System als WEB-Administrator an und rufen Sie sich den Menü-Punkt ► **Konfiguration** ► **Benutzerverwaltung** auf.

Wählen Sie die Zeile mit dem Benutzer, dessen Öffnungsvorgänge von der Zentrale freigegeben werden sollen. Der Benutzer benötigt einen ganz normale Öffnungsberechtigung (z.B. PIN Code). Sobald die „Fernfreigabe“ aktiviert ist, benötigt der Benutzer dann eine Freigabe, um das Schloss-System mit seinen Berechtigungen öffnen zu können. *Beispiel:*

Id-Nr	Benutzer	Anrede/ Typ	Name	Vorname					Web-Master	PIN Code	Chipkarte	Biometrie	min. 2 aus X	Schließer	ohne Zeitverz.	2-Augen	EMA	Fernfreigabe
10000	1	Herr	Mustermann	Max					✗	✓	✗	✗	✗	✗	✗	✗	✗	✗

Aktivieren Sie die Fernfreigabe des Benutzers. Die Berechtigung wechselt von nicht vergeben (nicht aktiv) [✗] auf ► vergeben (aktiv) [✔]. *Beispiel:*

Id-Nr	Benutzer	Anrede/ Typ	Name	Vorname		Web-Master	PIN Code	Chipkarte	Biometrie	min. 2 aus X	Schließer	ohne Zeitverz.	2-Augen	EMA	Fernfreigabe
10000	1	Herr	Mustermann	Max		✗	✔	✗	✗	✗	✗	✗	✗	✗	✔

Der Benutzer kann jetzt nicht mehr (allein) das Schloss-System öffnen. Wenn der Benutzer nun vor Ort ist und sich in der Zentrale meldet und darum bittet, das Schloss-System öffnen zu dürfen, dann vergeben Sie unter dem Menüpunkt ► **Steuerung** ► **Fernfreigabe** die entsprechende Freigabe.

25. Fernfreigabe: Freigeben eines Benutzers aus der Zentrale

Der Benutzer welcher aus der Ferne freigegeben werden soll, wurde unter ► **Konfiguration** ► **Benutzerverwaltung** für die „**Fernfreigabe**“ aktiviert (siehe vorheriger Abschnitt).

Es können nun alle Benutzer denen einen Passwort für den Web-Login zugewiesen wurde, Freigaben erteilen. Es ist nicht zwingend notwendig, dass jene Benutzer eine Web-Master Berechtigung haben.

Beispiel: Anlegen eines Benutzers, der Freigaben erteilen darf, aber kein Web-Master ist.

Der Benutzer wurde unter ► **Konfiguration** ► **Benutzerverwaltung** angelegt.
Der Benutzer benötigt keine Schloss-Benutzer ID.

Bearbeiten Sie die ► Authentifizierung [ ] des neuen Benutzers und aktivieren Sie ► **Web Login** und vergeben Sie ein Passwort für den Benutzer.

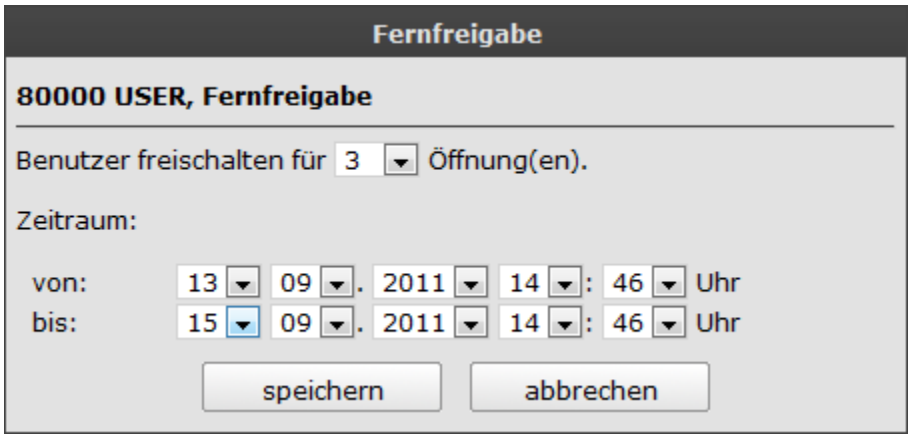
Id-Nr	Benutzer	Anrede/ Typ	Name	Vorname		Web-Master	PIN Code	Chipkarte	Biometrie	min. 2 aus X	Schließer	ohne Zeitverz.	2-Augen	EMA	Fernfreigabe
10015	---	System	Fernfreigabe	WEB		✗									

Wenn sich ein für den Web-Login berechtigter Benutzer mit seiner ID und seinem Passwort am Web-Interface anmeldet, kann unter dem Menüpunkt ► **Steuerung** ► **Fernfreigabe** ein Benutzer zentral freigeschaltet werden.

Id-Nr	Benutzer	Anrede	Name	Vorname	
80000	2	Beispiel	USER	Fernfreigabe	

Über den Button [ ] kann eine mehrfache Fernfreigabe für den Benutzer erteilt werden. Der Benutzer wird berechtigt in einem definierten Zeitraum eine definierte Anzahl von Öffnungen durchzuführen. Nach Ablauf des Zeitraums oder nach Ablauf der Öffnungen benötigt der Benutzer erneut eiune Freigabe.

In diesem Beispiel kann der Benutzer 3 Öffnungen im Zeitraum 13.09. (14.46 Uhr) bis 15.09. (14.46 Uhr) durchführen.



Über den Button [ ] kann eine einfache Fernfreigabe für den Benutzer erteilt werden. Der Benutzer wird für das einmalige Öffnen des Schlosses innerhalb der nächsten 30 Minuten berechtigt. Nach Ablauf der 30 Minuten oder nach der einmaligen Öffnung benötigt der Benutzer eine erneute Freigabe.

Wichtig bei der einmaligen Fernfreigabe [ ]: Der Benutzer wird bei einem 2-Schloss-System (z.B. CEN V – Recycler) immer für Schloss 2 berechtigt, es sei denn, der Benutzer hat in der Benutzerverwaltung keine Berechtigung für das zweite Schloss erhalten. In diesem Fall wird der Benutzer dann für das Schloss 1 berechtigt.

Kontaktdaten und Support

SAFECOR GmbH
Buchenring 55
22359 Hamburg
Deutschland

www.ProtectMaster.de
Kontakt@ProtectMaster.de

Tel: +49(0)40-866874-10
Fax: +49(0)40-866874-12