



ONE SYSTEM SECURE | Die PLUS-Lösung

Version: 1.17.
Anleitung: 1.7

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

Systempartner:

OSsecure Anleitung

Autor:

JPS/ KTS

Info & Feedback:

Doku@OSsecure.de

Beschreibung der Administrationsmöglichkeiten für die Berechtigung einzelner Software-Funktionen

Im Handbuch werden Fragen nach den Berechtigungen unter dem Punkt „Berechtigungskonzept“ erläutert. Wenn Sie sich als Administrator im System anmelden, können Sie sich unter dem Menü ► Konfiguration ► Berechtigungskonzept die bei Ihnen angelegten Berechtigungsgruppen aufrufen. Sie können beliebig viele weitere Berechtigungsgruppen anlegen und diese so auf die bei Ihnen im Hause gängigen Bezeichnungen (Namen) und Organisationsstruktur anpassen.

Neues Berechtigungskonzept anlegen 

Berechtigungskonzept			
• Sicherungssysteme			
• Kassenschleuse			
• Depotnutzer			
• Kassenmitarbeiter			
• Revisor			
• Verwaltung			
• Administrator			

Wenn es sich bei der im Berechtigungskonzept angelegten Gruppe um einen „Bediener“ handelt, welcher keine zusätzlichen Verwaltungs-Funktionen in der Software freigeschaltet bekommen soll, sondern ausschließlich Nutzer / Bediener der Multisafes / Schlösser / Kassenschleusen sein soll, dann müssen lediglich die jeweiligen Geräte zugeordnet werden, welche von der Gruppe bedient werden sollen. Die Zuordnung der Geräte zu einer Bedienergruppe konfigurieren Sie über den Button  (Kette) in den Stammdaten und unter dem Punkt Geräte verwalten.

Wenn es sich bei der im Berechtigungskonzept angelegten Gruppe um einen „Administrator“ handelt, welcher zusätzliche Verwaltungs-Funktionen in der Software freigeschaltet bekommen soll, dann können Sie diese Funktionen im Menü ► Konfiguration ► Programmfunktionen aktivieren.

Administratoren können das System verwalten, neue Bediener anlegen und Berechtigungen vergeben. Bediener können die Geräte (z.B. Kassenschleuse, Türzugänge, Tresorschlösser, Tagestresore) „lediglich“ bedienen. Sie verfügen aber über keine zusätzlichen administrativen Rechte im System.

Programmfunktion	
Bearbeiten der Stamm und Authentifizierungsdaten	
Geräte verwalten	
Bearbeiten des Berechtigungskonzeptes	
Systembackup erstellen	
Einsicht von Synchronisationsfehlern	
Einspielen von Systemupdates	
System herunterfahren	
Programmfunktionen bearbeiten	
Logdateien einsehen	
Alarm deaktivieren	
Reset der Controllerkarte	
Fingerscanner Verwalten	
Systemzeit einstellen	
Netzwerk einstellen	
BioEntry Verwalten	
Kurzfreischaltung	
System einstellen	
Depotfachverwaltung	
Berechtigung für Benutzer von Depotfächern	
Pin - User Berechtigung	
TwinLock BioPIN Verwalten	
TwinLock BioPIN Master	
TwinLock BioPIN freie PIN-Generierung	
Exports - User Berechtigung	
Pin - User Berechtigung	

Beispiel:

Sie legen sich im Berechtigungskonzept eine neue Gruppe „Netzwerkadministrator“ an.

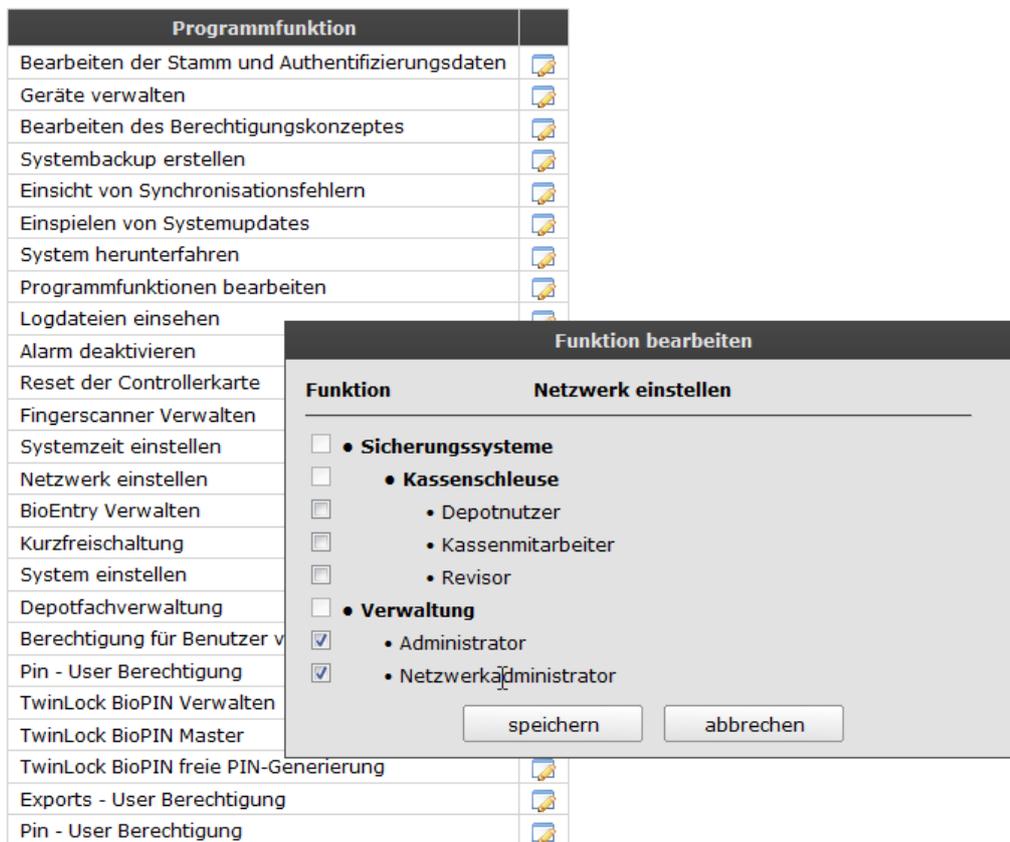
Neues Berechtigungskonzept anlegen

Berechtigungskonzept			
• Sicherungssysteme			
• Kassenschleuse			
• Depotnutzer			
• Kassenmitarbeiter			
• Revisor			
• Verwaltung			
• Administrator			

Berechtigungskonzept bearbeiten

Bezeichnung	<input type="text" value="Netzwerkadministrator"/>
Elternrolle	• Verwaltung ▼
Gültigkeit	<input type="checkbox"/> Gültigkeitszeiträume aktivieren Montag ▼ 00 ▼ : 00 ▼ : 00 ▼ Uhr bis 00 ▼ : 00 ▼ : 00 ▼ Uhr Hinzufügen
Zur Zeit hinterlegte Gültigkeiten:	
--- keine Zeiträume eingetragen ---	
speichern abbrechen	

Anschließend geben Sie der neuen Gruppe Netzwerkadministrator im Menü ► Konfiguration ► Programmfunktionen die Berechtigung „Netzwerk einstellen“. Personen/Mitarbeiter, welche jetzt im Menü ► Konfiguration ► Stammdaten jener neuen Gruppe zugeordnet werden, können im System nun die Netzwerkdaten ändern/einstellen.



Die folgende Beschreibung erläutert die Programmfunktionen im System, welche Sie optional (auch) anderen Berechtigungsgruppen zuordnen können. Standardmäßig sind jene Berechtigungen der Gruppe „Administrator“ und „Systemadministrator“ zugeordnet. Diese beiden Administratorengruppen unterscheiden sich lediglich dahingehend, dass der Gruppe „Administrator“ auch Programmfunktionen entzogen werden können. Damit man sich nicht versehentlich vom System aussperrt, weil sich der Administrator z.B. versehentlich notwendige Rechte entzogen hat, sind beim Systemadministrator bestimmte „notwendige“ Berechtigungen nicht löschar.

Programmfunktion	Beschreibung
Bearbeiten der Stamm und Authentifizierungsdaten	Berechtigung für das Anlegen von Stammdaten und das Erfassen von biometrischen Daten, sowie PIN-Berechtigungen, RFID Karten und weiteren Authentifizierungsdaten.
Geräte verwalten	Berechtigung für das Zuordnen von Geräten (z.B. Kassenschleuse, Multisafe, Zugang, Schlösser), welche von im Berechtigungskonzept hinterlegten Gruppen/ Rollen (z.B. Kassenmitarbeiter) benutzt werden dürfen.
Bearbeiten des Berechtigungskonzeptes	Berechtigung für das Anlegen oder Löschen von Berechtigungsgruppen
Systembackup erstellen	Berechtigung für das Erstellen einer separaten (zusätzlichen) Datensicherung
Einsicht von Synchronisationsfehlern	Berechtigung für das Einsehen des Synchronisationsstatus

Einspielen von Systemupdates	Berechtigung für das Einspielen von Systemupdates (diese Funktion steht in neueren Systemen nicht mehr zur Verfügung)
System herunterfahren	Berechtigung für das softwareseitige Neustarten eines Systems (Kassenschleuse, Multisafe, Zugang, Schlösser)
Programmfunktionen bearbeiten	Berechtigung für das Zuweisen von Programmfunktionen zu einer Berechtigungsgruppe
Logdateien einsehen	Berechtigung für das Einsehen von Logdaten
Alarm deaktivieren	Berechtigung für das Rücksetzen eines Alarms (betrifft nur bestimmte Geräte und Steuerplatinen). Eine Kassenschleuse, Multisafe, Zugang, Schlösser muss nach einer Alarmabsetzung nicht zurückgesetzt werden.
Reset der Controllerkarte	Berechtigung für einen Reset einer Controllerkarte (betrifft nur bestimmte Geräte und Steuerplatinen, wie z.B. Tagestresore älterer Bauart).
Fingerscanner Verwalten	Berechtigung für die Konfiguration bestimmter Fingerscanner (z.B. Auftischvariante, welche Bei Whitecard-Dispensern eingesetzt wird).
Systemzeit einstellen	Berechtigung für das Einstellen der Uhrzeit
Netzwerk einstellen	Berechtigung für das Einstellen der Netzwerkdaten
BioEntry Verwalten	Berechtigung für das Einstellen von biometrischen Türzugängen
Kurzfreischaltung	Berechtigung für das Sonderrecht „Kurzfreischaltung“, was bei bestimmten Prozessen für die gesonderte Berechtigung externer Personen verwendet werden kann (spezielle Service- oder Cashhandling-Prozesse).
System einstellen	Berechtigung für die Konfiguration diverser Systemparameter
Depotfachverwaltung	Berechtigung für das Verwalten von Depotfächern (z.B. Vorbestelltes Geld bei Tagestresoren).
Berechtigung für Benutzer von Depotfächern	Berechtigung für die Benutzer von Depotfächern
Pin - User Berechtigung	Systemberechtigung für das automatische Anlegen von PIN Code Berechtigungen über das Display eine PIN bedienten Tagestresors (Admin kann über Fach 0 User ohne Webinterface anlegen). Der neue User bekommt dann autom. alle Berechtigungsgruppen zugewiesen, welche jene Programmfunktion enthalten.
TwinLock BioPIN Verwalten	Berechtigung für das Verwalten von BioPINs für die zusätzliche biometrische Absicherung von Hochsicherheitsschlössern der Baureihe TwinLock WTU.
TwinLock BioPIN Master	Berechtigung für das Verwalten von Einmalmaster-TANs für Hochsicherheitsschlössern der Baureihe TwinLock WTU.
TwinLock BioPIN freie PIN-Generierung	Berechtigung für das Wählen eines beliebigen Zeitraums für das Erstellen von BioPINs für Hochsicherheitsschlössern der Baureihe TwinLock WTU.
Exports - User Berechtigung	Berechtigung für das Exportieren (CVS-Export) der im System hinterlegten Berechtigungen in einem Zentralsystem (Windows).

Im Auslieferungsstand ist das System mit einer administrativen Rolle (Administrator und

Systemadministrator) und verschiedenen Benutzerrollen konfiguriert. Sofern aus organisatorischen Gründen kein anderes Berechtigungskonzept gewünscht ist, müssen auch keine gesonderten Berechtigungsgruppen angelegt werden.