



ONE SYSTEM SECURE | Die PLUS-Lösung

Version: 1.16.14
Anleitung: 1.1

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

Systempartner:

OSsecure Anleitung			
Autor:	JPS/ KTS	Info & Feedback:	Doku@OSsecure.de

Inhaltsverzeichnis

OSsecure Einleitung	3
OSsecure © Urheberrechtshinweis	3
Zertifizierungen nach VBG, UVV-Kassen (BGV C9), BGI/GUV-I 819	3
Hinweise zur Kassensicherung	4
Inbetriebnahme des Systems	5
Anschluss der Gerätekomponenten	5
Anmeldung am OSsecurePlug	6
Einen neuen Administrator einrichten	7
Biometrischen Fingerprint-Scanner einrichten	9
Status und Funktion des Fingerprint-Scanners überprüfen	10
Bedienung des Fingerprint-Netzwerkscanners	11

OSsecure Einleitung

Wir beglückwünschen Sie zu Ihrer Entscheidung, die OSsecure-Lösungen einzusetzen. OSsecure ist ein biometrisches Identifikations- und Authentisierungssystem mit einer zuverlässigen Personenerkennung. Mit OSsecure werden Berechtigungen und Zugänge zentral verwaltet und unter Geräten und Systemen automatisch synchronisiert. Ein Benutzer, der einmal am System angelernt wurde, kann auf alles zugreifen, wofür er berechtigt wurde, ohne jedes Mal neu angelernt werden zu müssen. Die Benutzer müssen sich nicht unterschiedliche Passwörter oder Codes merken, und der organisatorische Aufwand für die Verwaltung von Berechtigungen wird auf ein Minimum reduziert. Die klassische Schlüsselverwaltung kann entfallen.

Für weitere Informationen lesen Sie bitte auch online unter www.OSsecure.de oder sprechen Sie Ihren Vertriebsmitarbeiter an.

Bei Anregungen und Verbesserungsvorschlägen zu dieser Anleitung oder zum Funktionsumfang, sowie der Bedienung des OSsecure-Systems freuen wir uns über Ihre Rückmeldung unter Doku@OSsecure.de.

OSsecure © Urheberrechtshinweis

Alle Inhalte dieses Handbuches, insbesondere Texte und Grafiken, sowie spezielle Funktionen des OSsecure-Systems sind urheberrechtlich geschützt (Copyright). Das Urheberrecht liegt, soweit nicht ausdrücklich anders gekennzeichnet, bei OSsecure. Bitte fragen Sie uns unter Kontakt@OSsecure.de, falls Sie die Inhalte dieses Handbuches verwenden möchten.

Wer gegen das Urheberrecht verstößt (z.B. die Inhalte unerlaubt kopiert oder manipuliert), macht sich gem. § 106 ff Urhebergesetz strafbar. Er wird zudem kostenpflichtig abgemahnt und muss Schadensersatz leisten. Kopien von Inhalten können ohne großen Aufwand nachverfolgt werden.

© OSsecure 11.05.2009

Die Verfasser behalten sich das Recht vor, das vorliegende Handbuch oder Teile des Inhalts, ohne vorherige Ankündigung zu ändern oder zu ergänzen.

Zertifizierungen nach VBG, UVV-Kassen (BGV C9), BGI/GUV-I 819

Das OSsecure-System ist von der Verwaltungs-Berufsgenossenschaft (VBG), dem Fachausschuss Verwaltung der Berufsgenossenschaftlichen Zentrale für Sicherheit und Gesundheit – BGZ des Hauptverbandes der gewerblichen Berufsgenossenschaften (Sachgebiet Kassen) zertifiziert. Die **Eignungsbescheinigung** bestätigt, dass OSsecure, als Komponente in Kassensicherungskonzepten mit biometrischen Systemen, insbesondere in der PLUS-Lösung oder bei der durchschusshemmenden Kasse mit biometrisch überwachter Zugangsschleuse, eingesetzt werden kann.



Die Konfiguration der Software muss dabei so erfolgen, dass die Anforderungen der UVV-Kassen (BGV C9) i.V.m. den BGI/GUV-I 819-2 und BGI/GUV-I 819-3 eingehalten werden.

Hinweise zur Kassensicherung

Bitte beachten Sie, dass auf die besondere Funktionsweise einer bestimmten Kassensicherung (z.B. PLUS-Stelle) mit geeigneten Hinweisschildern gut sichtbar am Eingang, an den Bedienerplätzen und an den Geräten hingewiesen wird (vergl. UVV-Kasse, GUV/BGI).

Beispiele:

Automatengesichert
Barauszahlungen durch einen Mitarbeiter
allein nicht möglich.

Automatengesichert
Barauszahlungen nur durch zwei Mitarbeiter
nach biometrischer Identifizierung.

Multisafes welche über ein biometrisches System gesteuert werden, aber weiterhin mit einem Tastenfeld einem Display ausgestattet sind, könnten suggerieren, dass eine Bedienung des Gerätes mittels PIN-Code weiterhin möglich ist. Es ist daher bei diesen Geräten optional möglich, das Display stillzulegen oder die Display-Anzeige auszublenden. **Beachten Sie daher unbedingt die Beschilderung Ihrer Kassensicherung, um Gefahrensituationen vorzubeugen.**

Bitte beachten Sie weiterhin, dass die Arbeitsverfahren und Arbeitsabläufe in den Geschäftsstellen einwandfrei gestaltet, bzw. geregelt sind und die Unterweisungen der Geschäftsstellenmitarbeiter vollständig ist.

Für den Anlernprozess von Mitarbeiter (biometrische Erfassung) gelten besondere Bestimmungen. **Bitte informieren Sie sich bei Ihrem zuständigen Vertriebsmitarbeiter, welche Regeln vor dem Hintergrund der UVV-Kassen zwingen Berücksichtigung finden müssen.**

Aufgrund der Vielzahl von Konfigurations- und Einsatzmöglichkeiten kann in dieser Dokumentation nicht weiter auf jeden spezifischen Anwendungsfall eingegangen werden. So ist es beispielsweise erforderlich, dass der Administrator bei der biometrischen Erfassung der Mitarbeiters nur dann alle 10 Finger der Mitarbeiter erfasst, wenn jene Mitarbeiter in der Geschäftsstelle vor Ort auch Kunden mit in das biometrische System aufnehmen sollen, um z.B. mit dem Kunden zusammen vorbestelltes Geld aus dem Multisafe auszuzahlen. Ist die biometrische Erfassung von Kunden nicht gewünscht, so wäre das Anlernen von einem oder wenigen Fingern der Mitarbeiter ausreichend. Weiterhin gelten unterschiedliche Regelungen für den eigentlichen Anlernprozess.

Die Anwendung und die Konfiguration der Software muss so erfolgen, dass die Anforderungen der UVV-Kassen (BGV C9) i.V.m. den BGI/GUV-I 819-2 und BGI/GUV-I 819-3 eingehalten werden.

Inbetriebnahme des Systems

Anschluss der Gerätekomponenten

Diese Anleitung beschreibt den Anschluss des OSsecurePlug. Der Plug ist eine Erweiterung für den Betrieb eines biometrischen Fingerprint Scanners im Netzwerk.

- ▶ Schließen Sie das Gerät mit dem Netzkabel (Stromkabel) an einer geerdeten 220V Steckdose an.
- ▶ Schließen Sie ein Netzkabel (CAT5) an den Plug an.
- ▶ Schließen Sie den USB-Fingerprint-Scanner an den Plug an.

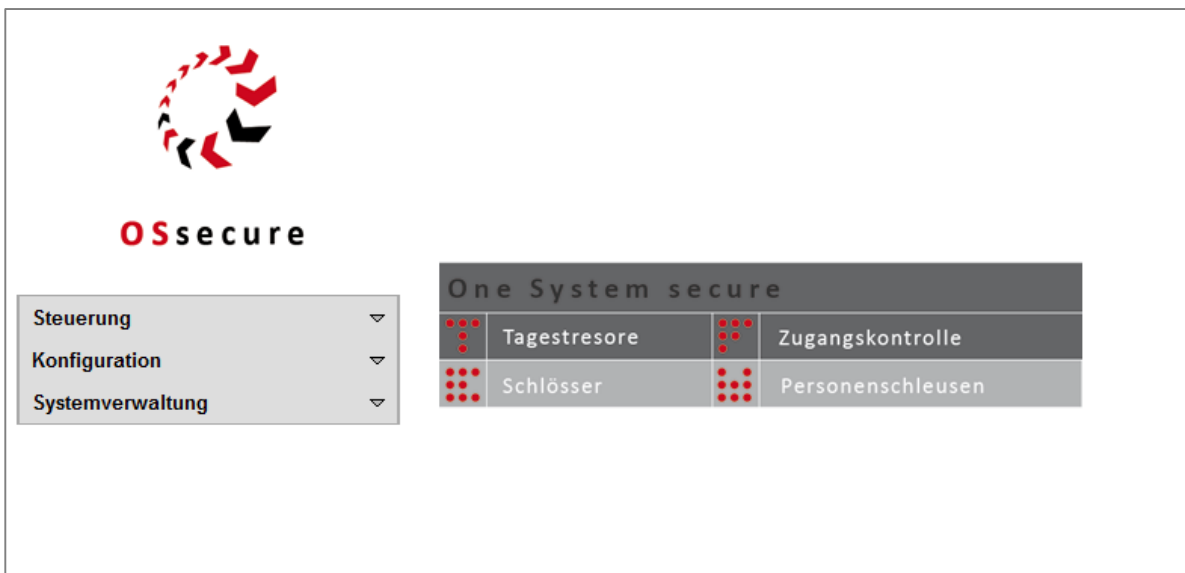
Bei der Erstinstallation müssen Sie die Netzwerkadresse des Gerätes für den Betrieb im Bank-Netzwerk einstellen. Standardmäßig wird der Plug mit folgender IP-Adresse ausgeliefert:

IP-Adresse: **192.168.1.30**
 Subnetmask: 255.255.255.0

Verbinden Sie das Netzkabel mit dem Plug und Ihrem Rechner. Stellen Sie die IP-Adresse Ihres Rechners auf den Adressbereich des Plug (Netzwerkscanner) ein (z.B. 192.168.1.20).

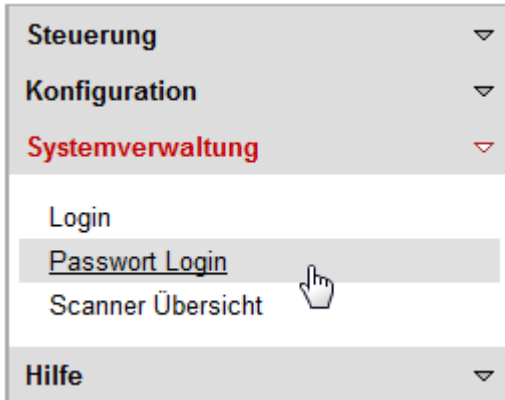
Rufen Sie sich die IP-Adresse des Plugs in Ihrem Webbrowser auf (<http://192.168.1.30>).

Sie sehen die folgende Begrüßungsseite.



Anmeldung am OSsecurePlug

Stellen Sie eine Verbindung zum Gerät her (siehe Abschnitt „Anschluss der Gerätekomponenten“)



Bitte melden Sie sich nach der Inbetriebnahme des Gerätes für die Erstanmeldung mit den Ihnen zugeschickten Anmeldedaten an. Diese bestehen aus einer Identifikationsnummer und einem Passwort.

Beispiel:
ID-Nummer: 1000
Passwort: sysadmin

Sollten Ihnen keine Login Daten für die Erstanmeldung vorliegen, so kontaktieren Sie uns bitte, damit wir Ihnen die Daten nennen können.

Bitte geben Sie die ID-Nummer und das Passwort ein

ID-Nummer	<input style="width: 80%;" type="text" value="100"/>
Passwort	<input style="width: 80%;" type="password" value="....."/>
<input style="margin-right: 20px;" type="button" value="OK"/> <input type="button" value="abbrechen"/>	

► Nach erfolgreicher Anmeldung, sollten Sie sich zunächst einen Administrator-Bediener anlegen. Den für die Erstanmeldung verwendeten Benutzer löschen Sie bitte erst, wenn Sie weitere Bediener und/ oder Administratoren eingerichtet haben und die Funktion der Benutzerrechte mehrfach getestet haben. Nachdem Sie den für die Erstanmeldung verwendeten Benutzer gelöscht haben, besteht telefonisch keine Möglichkeit, diesen zu reaktivieren oder zu „umgehen“. Achten Sie daher dringend darauf, dass Sie zu diesem Zeitpunkt bereits mit einem eingerichteten Benutzer über Administrator-Rechte verfügen, da es andernfalls möglich ist, dass Sie sich vom OSsecure-System aussperren.



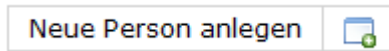
Einen neuen Administrator einrichten

- Steuerung ▾
- Konfiguration** ▾
- Stammdatenverwaltung 
- Depotfachverwaltung
- Geräte verwalten
- Berechtigungskonzept
- Programmfunktionen verwalten
- Systemverwaltung ▾
- Hilfe ▾

Melden Sie sich am OSsecurePlug als Administrator an (*siehe Punkt: Anmeldung am OSsecurePlug*)

Menü ► **[Konfiguration]** ► **[Stammdatenverwaltung]**

Neuen Benutzer anlegen ► **[Neue Person anlegen]**



Es erscheint der Dialog "Person bearbeiten". Hier können Sie alle relevanten Personendaten, wie Anrede, Name und ID-Nummer festlegen. **Die Identifikationsnummer muss eingegeben werden.** Sie entspricht der Benutzernummer und kann eine beliebige Zahl mit neun Stellen sein.

Person bearbeiten

Anrede	<input type="text" value="Herr"/>
Vorname	<input type="text" value="Max"/>
Nachname	<input type="text" value="Mustermann"/>
Id-Nr	<input type="text" value="1234567890"/>
Beginn	<input type="text" value="02"/> ▾ . <input type="text" value="05"/> ▾ . <input type="text" value="2009"/> ▾ <input type="text" value="08"/> ▾ : <input type="text" value="00"/> ▾ : <input type="text" value="00"/> ▾
Ende	<input type="text" value="31"/> ▾ . <input type="text" value="12"/> ▾ . <input type="text" value="2176"/> ▾ <input type="text" value="00"/> ▾ : <input type="text" value="00"/> ▾ : <input type="text" value="00"/> ▾
<input type="checkbox"/> Einmalöffnung	
<input type="button" value="speichern"/> <input type="button" value="abbrechen"/>	

► Hinterlegen Sie Anrede, Namen und Vornamen, sowie eine ID-Nummer für den neuen Benutzer.






► Das Beginndatum muss nicht verändert werden, es sei denn, Sie möchten, dass der Benutzer erst ab oder nur bis zu einem bestimmten Zeitpunkt aktiv ist. Außerhalb des Zeitraums ist der Benutzer deaktiviert (ohne Rechte).

► Der Haken bei [Einmalöffnung] ist für den Betrieb des Plugs nicht relevant.


Suchen Sie anschließend den neu angelegten Benutzer aus der Übersicht heraus und fahren Sie mit der Konfiguration des neuen Benutzers fort. Neben dem Benutzer sehen Sie folgende Symbole:




Hinter den Symbolen verbergen sich die folgenden Funktionen und Menüs:

1		2		3		4		6	
Bearbeiten		Passwort anlegen		Löschen		Berechtigungen		Aktivität	
Benutzerdaten (z.B. Name, Vorname) bearbeiten.		Art der Benutzer-Identifizierung bearbeiten und Fingerprints anlernen.		Benutzer löschen.		Benutzerrechte bearbeiten/ einstellen.		Benutzer für einen bestimmten Zeitraum aktivieren/ deaktivieren.	

Vergeben Sie unter dem Punkt „Berechtigungen“ eine Berechtigung für Ihren Benutzer.

► Symbol **Berechtigungen** [] ► Es öffnet sich der Dialog, um die Berechtigungen zu bearbeiten. Hier vergeben Sie sich bitte die Rechte für **Administrator** und **System Administrator**. Schließen Sie den Dialog mit „speichern“ ab.

Vergeben Sie unter dem Punkt „Passwort anlegen“ ein Passwort für Ihren Benutzer:

► Symbol Passwort anlegen [] ► Es startet der Dialog für die Passwortvergabe.

Unter dem Punkt ► **Passwort bearbeiten** (Der Benutzer darf sich per Passwort authentifizieren (Web - Login) setzen Sie bitte einen Haken.

Sie erhalten folgende Meldung mit Ihrem Initialpasswort. Kopieren und notieren Sie sich das Passwort.



Sie können das Passwort ändern, indem Sie sich unter Systemverwaltung abmelden (Logout) und mit der Identifikationsnummer des neu angelegten Benutzers und des Initialpassworts anmelden. Anschließend gehen Sie unter ► Systemverwaltung ► Passwort ändern.

Biometrischen Fingerprint-Scanner einrichten

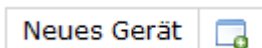
Schließen Sie den Um den biometrischen Fingerprint-Scanner einzurichten, gehen Sie bitte wie folgt vor.

► Schließen Sie den USB-Fingerprint-Scanner an den Plug an. Stecken Sie das USB-Kabel des Scanners in die USB-Buchse des Plug.

Melden Sie sich im Webbrowser als Administrator an dem Plug an.

Menü ► **[Konfiguration]** ► **[Geräte verwalten]** Es öffnet sich eine Übersicht und Sie haben die Möglichkeit ein neues Gerät anzulegen.

Klicken Sie bitte auf das folgende Symbol:



Es öffnet sich der Dialog für die Geräteeinstellungen:

Gerät bearbeiten

Gerätebezeichnung	<input style="width: 95%;" type="text"/>
Zieladresse	<input style="width: 95%;" type="text"/>

► Tragen Sie einen Namen für den Scanner ein. Beispiel: *Netzwerkscanner Servicetresen*.

► Geben Sie als Zieladresse die IP-Adresse oder den Hostnamen des OSsecure-Systems ein, mit welchem der Netzwerkscanner (Plug) kommunizieren soll (z.B. der Tagestresor).

Schließen Sie den Dialog mit „**speichern**“ ab.

Aktivieren Sie jetzt unter dem Menü Steuerung das Gerät:

Menü ► **[Steuerung]** ► **[Plug]**. Hier sollte das Zielgerät mit einem grünen Haken und der Statusmeldung „letzter Ping: OK“ angezeigt werden. Klicken Sie zur Aktivierung auf das OSsecure-System (*Beispiel: Tagestresor GS 660 links*). Die Seite aktualisiert sich nicht automatisch. Nach einer kurzen Wartezeit (max. 60 Sek.) können Sie die Seite neu laden (Taste F5).

Auswahl Zielgerät
Tagestresor GS 660 links (192.168.0.27)  letzter Ping: OK
Tagestresor GS 660 rechts (192.168.0.83)

Status und Funktion des Fingerprint-Scanners überprüfen

Status des Scanners prüfen:

Menü ► [Systemverwaltung] ► [Scanner Übersicht]. Hier sollte unter dem Punkt „Aktive USB- und Netzwerkscanner“ der USB-Fingerprint Scanner mit dem Status „OK“ angezeigt werden.

Wenn der Scanner dort nicht angezeigt wird oder der Status fehlerhaft ist, dann überprüfen Sie bitte die Kabel- und Steckverbindung zwischen dem Fingerprint-Scanner und dem Plug. Sollten nach dem Überprüfen der Kabelverbindung keine Statusänderung erfolgen, wählen Sie bitte den Punkt „**Usbports zurücksetzen**“ oder wenden Sie sich an den Support, da die Lizenzierung des Scanner evtl. fehlerhaft ist.

Verbindung zum OSsecure-System überprüfen:

Menü ► [Steuerung] ► [Plug]. Hier sollte das Zielgerät mit einem grünen Haken und der Statusmeldung „letzter Ping: OK“ angezeigt werden.

Wenn das Gerät dort nicht mit einem grünen Haken aktiv ist, klicken Sie mit der Maus auf das OSsecure-System, mit welchem der Scanner kommunizieren soll. Die Seite aktualisiert sich nicht automatisch. Nach einer kurzen Wartezeit (max. 60 Sek.) können Sie die Seite neu laden (Taste F5).



Wenn Sie eine fehlerhafte Verbindung angezeigt bekommen (*siehe Beispiel: „letzter Ping: keine Verbindung“*), überprüfen Sie bitte die Zieladresse des OSsecure-Systems, welche Sie unter dem Punkt „Biometrischen Fingerprint-Scanner einrichten“ hinterlegt haben. Das OSsecure-System sollte eingeschaltet und erreichbar sein. Rufen Sie sich die IP-Adresse des OSsecure-System zur Überprüfung im Webbrowser auf.

Verbindung am OSsecure-System überprüfen:

Rufen Sie sich Ihr OSsecure-System (nicht den OSsecurePlug) im Webbrowser auf. Überprüfen Sie, ob der OSsecurePlug eine Verbindung zum OSsecure-System hat.

Menü ► [Systemverwaltung] ► [Scanner Übersicht].

Sie sollten jetzt alle Scanner aufgeführt sehen, welche mit dem OSsecure-System kommunizieren. Unter dem Punkt OSSConnect Scanner sollte der OSsecurePlug mit dem Status OK aufgeführt sein. Beispiel:

OSSConnect Scanner

Host	letzter Kontakt	Angeschlossene Scanner
PLUG	18.08.2011 16:57:24	Futronic FS88: Ok

Wir der Plug nicht aufgeführt, überprüfen Sie bitte die Einstellungen der Zieladresse des OSsecurePlug.

Bedienung des Fingerprint-Netzwerkscanners

Wenn Sie den Netzwerk-Fingerprint-Scanner erfolgreich eingerichtet haben, der Status des Fingerprint-Scanners „OK“ anzeigt und Sie eine Verbindung zum OSsecure-System haben (siehe Punkt: „Status und Funktion des Fingerprint-Scanners überprüfen“), dann können Sie das Gerät bedienen.

Rufen Sie sich im Browser das OSsecure-System auf, welches Sie beim OSsecurePlug als Ziel-System (Zieladresse) hinterlegt haben.

Testen Sie die Funktion Ihres Netzwerkscanners, indem Sie versuchen ein Fach zu öffnen oder sich am System mittels biometrischer Identifizierung anzumelden.