



FleetCockpit Security Datenblatt (FSM)

1. Übersicht über die Fleet & Servicemanagement Software

Die Fleet & Servicemanagement (FSM) Software ist eine sichere, Windows basierte Softwarelösung, die in allen Netzwerkkumgebungen eingesetzt werden kann. FSM erfasst nur Daten von Druck- bzw. Multifunktionssysteme, die für das Management einer Druckumgebung wichtig sind. Persönliche Daten oder Benutzerinformationen sind hiervon stets ausgenommen.

Die Fleet & Servicemanagement Software besteht aus zwei Teilen, der Fleet & Servicemanagement Client Software, die zur Erfassung, Auslesung und Überwachung der Druck- und Multifunktionssysteme des Endkunden dient, und der Fleet & Servicemanagement Server Software, die die erfassten Daten von der FSM Client Software empfängt, in einer zentralen Datenbank speichert, und die Browser-basierte Weboberfläche zur Ansicht der Daten, sowie den Berichtsgenerator und die Engine zur automatischen Reaktion der Software auf Ereignisse der Drucksysteme bereitstellt. Die FSM Client Software wird beim Endkunden installiert. Die erfassten Daten werden an einen zentralen FSM Server gesandt, der in einem von der Compass Gruppe und deren Entwicklungspartner und Hersteller der Software docuFORM, nach strengen, der Anwendung entsprechenden Sicherheitskriterien ausgewählten und beauftragten Rechenzentrum **in Deutschland** als FSM Hosting Service installiert ist.

2. Sicherheitsinformationen zur FSM Client Software

Die docuFORM Fleet & Servicemanagement (FSM) Client Software wird auf einem 32 oder 64 Bit Windows (Windows XP, Windows Vista, Windows 7, Windows 2003 Server, Windows 2008 Server) basierten PC im Netzwerk des Kunden installiert. Die FSM Client Software kann auch in virtuellen Umgebungen mit den o.A. Betriebssystemen installiert werden.

Die Kommunikation der FSM Client Software zu den überwachten Drucksystemen erfolgt über das standardisierte SNMP Protokoll. Die Weitergabe der von der FSM Client Software erfassten Informationen an die FSM Server Software kann auf zwei verschiedene, konfigurierbare Arten erfolgen:

- mittels E-Mail Übertragung
- mittels TCP/IP http oder https Übertragung

Die Kommunikation zwischen FSM Client Software und FSM Server Software erfolgt immer unidirektional von der FSM Client Software zur FSM Server Software. Es erfolgt keine Datenübertragung von der FSM Server Software zur FSM Client Software. Vom PC bzw. der virtuellen Umgebung, auf dem die FSM Client Software installiert wurde, muss ein Netzwerkzugriff per SNMP Protokoll auf die zu überwachenden Drucksysteme, sowie, je nach gewählter Kommunikationsart zum FSM Server, entweder ein Zugriff auf einen Mailserver zum Versand von E-Mails, oder die Möglichkeit zum Aufbau einer TCP/IP basierten XML-RPC oder http(s) basierten Verbindung zum FSM Server gegeben sein. Die entsprechenden Ports in lokalen Firewalls sind hierfür zu öffnen:

- Für SNMP Abfragen der Drucksysteme: Port 161 und 162
 - Für E-Mail Kommunikation: Port 25 zum Email Server
 - Für https basierte, gesicherte Kommunikation zum FSM Server: Port 443
 - Für http basierte Kommunikation zum FSM Server: Port 80
- oder



- Für die lokale Kommunikation zwischen dem FSM Client und der zugehörigen Web-basierten Konfigurationsoberfläche sind die Ports 52005 (TCP) und 52050 (UDP) zu öffnen.

3. Arbeitsweise der Software

Die FSM Client Software fragt über das SNMP Protokoll alle im Netzwerk eingebundenen Druck- und MFP Systeme zyklisch nach Seriennummer, Firmwarestand, Zählerständen, Toner- und Verbrauchsmaterial Level und Fehlerstatus ab und meldet diese Informationen zur Auswertung und Weiterverarbeitung an den FSM Server weiter. Informationen über Zählerstände, Toner-level und unkritische Druckerfehler werden in festen, definierbaren, Zeitintervallen an den Server weitergeleitet. Informationen über kritische Druckerfehler werden zeitnah (max. 10 min.) nach Erfassung an den FSM Server weitergeleitet. Bis zur Weiterleitung der erfassten Informationen an den Server werden alle von den überwachten Drucksystemen erfassten Informationen von der FSM Client Software in einer lokalen Datenbank zwischengespeichert.

Die Kommunikation zwischen FSM Client und Server Software ist **immer unidirektional** und erfolgt **nur vom Client zum Server**. Es findet keine Kommunikation vom Server in Richtung Client statt. Es können zur Kommunikation zwischen FSM Client und Server zwei Arten der Kommunikation eingestellt werden:

- Die Kommunikation über E-Mails, welche vom FSM Client an den Server mit verschlüsselten Inhalten versandt werden.
- Die Kommunikation über das gesicherte https oder das Standard http Internet Protokoll.

Mit diesen Konfigurationsvarianten kann allen Sicherheitsbedürfnissen von Anwendern Rechnung getragen werden. **Durch die mögliche Kommunikation zwischen FSM Client und Server per verschlüsselter E-Mail müssen zur Informationsübertragung keine Netzwerke der Kunden geöffnet oder Firewalls nach außen durchlässig gemacht werden. Alle bestehenden Sicherheitsvorkehrungen bei Kunden bleiben in vollem Umfang erhalten.** Es muss lediglich der FSM Client Software Zugriff auf einen EMail Server zum Versand von E-Mails an den FSM Server ermöglicht werden.

Die FSM Client Software erstellt keine Auswertungen über die von ihr erfassten Informationen der überwachten Drucksysteme. Diese werden alleine von der FSM Server Software bereitgestellt. Außer den von den Drucksystemen erfassten Informationen (siehe Abschnitt 4) werden keine Daten an die FSM Server Software weitergegeben.



4. Überblick über erfasste Daten und Informationen

Vom FSM Client werden die folgenden Informationen von den überwachten Druck- bzw. MFP Systemen abgefragt und, falls vom Gerät bereitgestellt, zyklisch an den Server gemeldet:

- Allgemeine Informationen über das Druck- bzw. MFP System, wie Modell, Name, Seriennummer, Firmwarelevel, TCP/IP Adresse bzw. DNS Name, MAC Adresse, Standortinformation und Kontakt
- Informationen zu den Eigenschaften der überwachten Systeme, wie Farbfähig, Duplexfähig, Finishing Optionen, Anzahl der Papierschächte etc.
- Zählerstände für Farb- und Schwarz/Weiß Drucke, Kopien und Faxe, Scans, sowie Sonderzähler soweit verfügbar.
- Tonerlevel aller im Gerät vorhandenen Toner, sowie die Status weiterer Verbrauchsmaterialien, falls vom Gerät gemeldet
- Alarm- und Fehlerzustände der Druck- und MFP Systeme
- Display-Meldungen der Druck- und MFP-Systeme

Es werden keinerlei Druckauftrags- oder Benutzerdaten erfasst. Weder Informationen über Namen bzw. Inhalte von Druckdateien noch über deren Erzeuger / Besitzer werden von der FSM Software erfasst und verarbeitet.

Welche Alarm- und Fehlerzustände der Druck- und MFP Systeme von der FSM Client Software erfasst und von der FSM Server Software ausgewertet werden sollen, lässt sich innerhalb der Fleet & Service Management Software genau konfigurieren.

Während unkritische Druckerzustände im Rahmen der Übermittlung von Zählerständen und Tonerlevel in konfigurierbaren Zeitabständen zyklisch vom Client an den Server übermittelt werden, werden kritische Fehler- und Alarmzustände sofort nach deren Erfassung vom Client an den Server gemeldet.

5. Optionales automatisches Update der Steuerdateien zur Auslesung der Systeme

Die Anweisungen zum Auslesen der Druck- und Multifunktionssysteme durch die FSM Client Software werden in gerätespezifischen Steuerdateien (PMD Dateien) hinterlegt. Für jeden Gerätetyp existiert eine solche PMD Datei, die der FSM Client Software mitteilt, an welcher Stelle der jeweiligen Management Information Base (MIB) der Systeme, die erwünschten Informationen über Zählerstände, Level der Verbrauchsmaterialien, etc. beim jeweiligen System per SNMP auszulesen sind. Das Installationspaket der FSM Client Software beinhaltet einen umfangreichen Pool solcher PMD Dateien für nahezu jedes gebräuchliche Drucksystem. Dennoch wird dieser Pool nahezu täglich um neue Drucksysteme ergänzt und erweitert.

Um die FSM Client Software bzgl. dieser PMD Dateien immer aktuell zu halten, kann innerhalb der FSM Client Software ein tägliches automatisches Update dieser PMD Dateien konfiguriert werden. Ist diese Option eingestellt, so stellt die FSM Client Software einmal täglich zum konfigurierten Zeitpunkt automatisch eine Internet Verbindung zu einem Server der docuFORM GmbH, Entwicklungspartner der Compass Gruppe, her und lädt von dort ein ZIP Archiv mit den aktuellen PMD Dateien herunter. Dieses Paket wird anschließend automatisch entpackt und in die FSM Client Software integriert.

Falls die automatische Online Aktualisierung der PMD Dateien nicht gewünscht wird, kann diese Aktualisierung auch jederzeit manuell vorgenommen werden.



6. Netzverkehr

Der von der FSM Client Software generierte Netzwerkverkehr zur Abfrage der Druck- bzw. Multifunktionssysteme ist minimal und variiert je nach der Anzahl der gescannten TCP/IP-Adressen.

Die Häufigkeit der Abfragen von Zählerständen und Ständen der Verbrauchsmaterialien lässt sich innerhalb der FSM Client Software im Bereich von 'alle 3 Stunden' bis zu 'einmal zum Quartalsende' konfigurieren. Die Abfrage der Drucksysteme auf Fehlerzustände erfolgt häufiger, da hierbei aber nur wenige Bytes übertragen werden, ist die hierdurch erzeugte Netzlast äußerst minimal.

7. Passwortgeschützter Zugriff auf die FSM Software

Der Zugriff auf die FSM Client und FSM Server Software erfolgt passwortgeschützt. In der Browser-basierten Weboberfläche der FSM Server Software existieren verschiedene Zugangslevel für Administratoren, Händler. Je nach Zugangslevel werden dem Anwender die dem Zugangslevel entsprechenden Rechte in der FSM Software eingeräumt.

8. HTTPS-Zugriff

Auf die Webseiten der Fleet & Servicemanagement Server Software kann mittels HTTPS Protokoll zugegriffen werden. Voraussetzung hierfür ist, dass der Webserver mit einem SSL-Sicherheitszertifikat ausgestattet worden ist.

Die Webseiten der FSM Client Software lassen sich nur vom lokalem PC bzw. der lokalen virtuellen Umgebung auf dem / der FSM Client Software installiert wurde, erreichen. Ein Zugriff von 'fernen' Browsern auf diese Seiten ist nicht möglich.

9. FSM Software Prüf- und -freigabeprozess

Jede größere und kleinere Softwarefreigabe durchläuft einen Qualitätssicherungsprozess, in dem mehrere Mitarbeiter des Herstellers die geänderten Systembereiche prüfen, um sicherzustellen, dass keine Beeinträchtigung der Sicherheit oder Funktionalität des Systems vorliegt. Größere Freigaben durchlaufen einen Beta-Freigabeprozess, in welchem das neue System auf Servern mit Testdaten parallel zu alten Systemen betrieben wird.

10. FSM Quellcodeschutz

Der Fleet & Servicemanagement Quellcode wird in einem gesicherten Revision Control System aufbewahrt, zu dem nur das Entwicklungsteam des Herstellers Zugang hat. Jede Änderung des Quellcodes wird nachverfolgt, einschließlich des Namens des Entwicklers, welcher die Änderung vornimmt, und des Grundes der Änderung.

Für weiterer Fragen und Informationen wenden Sie sich bitte an Ihren Partner der Compass Gruppe. www.compassgruppe.de