Computer•Schnittstellen•Peripherie GmbH

WIR SCHAFFEN IT-LÖSUNGEN

Informationen zur Sicherheit der docuFORM Mercury Fleet & Servicemanagement V9.x MPS Software

Inhaltsverzeichnis

1 Übersicht über die Fleet & Servicemanagement Software

Die docuFORM Mercury Fleet & Servicemanagement V9.x MPS Software ist eine sichere Softwarelösung, die in allen Netzwerkumgebungen eingesetzt werden kann. MPS erfasst nur diejenigen Daten des Druck- bzw. Multifunktionssystems, die für das Management einer Druckumgebung wichtig sind; persönliche Daten oder Benutzerinformationen sind hiervon stets ausgenommen.

Die Fleet & Servicemanagement MPS Software besteht aus zwei Teilen, der Fleet & Servicemanagement Client Software, die zur Erfassung, Auslesung und Überwachung der Druck- und Multifunktionssysteme des Anwenders dient, und der Fleet & Servicemanagement Server Software, die die erfassten Daten von der MPS 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.

Je nach gewünschtem Installationsszenario können die MPS Client und die MPS Server Software gemeinsam bei einem Anwender installiert werden, oder aber die MPS Client Software wird bei verschiedenen Anwendern installiert und meldet die erfassten Daten an einen zentralen MPS Server, der bei einem Händler, einer Händlerorganisation oder in einem Rechenzentrum als MPS Hosting Service installiert sein kann.

2 Sicherheitsinformationen zur MPS Client Software

Die docuFORM Fleet & Servicemanagement (MPS) Client Software wird auf einem 32 oder 64 Bit Windows (Windows 8, 8.1, 10), Windows 2012 Server, Windows 2012 R2 Server, Windows 2016 Server, Windows 2019 Server) basierten PC im Netzwerk des Kunden installiert. Die MPS Client Software kann auch in virtuellen Umgebungen mit den o.A. Betriebssystemen installiert werden.

Die Kommunikation der MPS Client Software zu den überwachten Drucksystemen erfolgt über das standardisierte SNMP V1, V2 oder V3 (ab MPS V7.20) Protokoll, wobei das SNMP V3 Protokoll eine sichere und verschlüsselte Kommunikation zwischen MPS Client Software und überwachten Drucksystemen ermöglicht.

Die Weitergabe der von der MPS Client Software erfassten Informationen an die MPS Server Software kann auf drei verschiedene, konfigurierbare Arten erfolgen:

- mittels direkter TCP/IP XML-RPC Übertragung
- mittels E-Mail Übertragung
- mittels TCP/IP http oder https Übertragung

Die Kommunikation zwischen MPS Client Software und MPS Server Software erfolgt immer unidirektional von der MPS Client Software zur MPS Server Software. Es erfolgt keine Datenübertragung von der MPS Server Software zur MPS Client Software.

Vom PC bzw. der virtuellen Umgebung, auf dem die MPS Client Software installiert wurde, muss ein Netzwerkzugriff per SNMP V1, V2 oder V3 (ab MPS V7.20) Protokoll auf die zu überwachenden Drucksysteme, sowie, je nach gewählter Kommunikationsart zum MPS

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 MPS Server gegeben sein. Die entsprechenden Ports in **lokalen** Firewalls sind hierfür zu öffnen:

- Für SNMPV1, V2 oder V3 (ab MPS V7.20) Abfragen der Drucksysteme: Port 161
- Für E-Mail Kommunikation: Port 25 zum Email Server
- Für https basierte, gesicherte Kommunikation zum MPS Server: Port 443
- Für http basierte Kommunikation zum MPS Server: Port 80

  oder

  Für TCP/IP XML-RPC Kommunikation zu einem **vor Ort installierten** MPS-Server: Port 52004

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

3 Arbeitsweise der Software

Die MPS Client Software fragt über das SNMP V1, V2 oder V3 (ab MPS V7.20) Protokoll alle im Netzwerk eingebundenen Druck- und MFP Systeme zyklisch nach Seriennummer, Firmwarestand, Zählerständen, Toner- und Verbrauchsmaterial Level und Fehlerstati ab und meldet diese Informationen zur Auswertung und Weiterverarbeitung an den MPS 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 MPS Server weitergeleitet. Bis zur Weiterleitung der erfassten Informationen an den Server werden alle von den überwachten Drucksystemen erfassten Informationen von der MPS Client Software in einer lokalen Datenbank zwischengespeichert.

Der MPS Server kann entweder ebenfalls intern beim Kunden, oder auch extern beim Händler oder bei einer Händlerorganisation installiert werden.

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

- Die Kommunikation über E-Mails, welche vom MPS Client an den Server mit verschlüsselten Inhalten versandt werden (empfohlen wenn MPS Client und Server an verschiedenen Standorten bzw. innerhalb verschiedener Netzwerke installiert sind).

- Die Kommunikation über ein spezielles TCP/IP XML-RPC Protokoll mit verschlüsseltem Datenaustausch (beispielsweise wenn MPS Client und Server am selben Standort bzw. im selben Netzwerk installiert sind).
- 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 MPS 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 MPS Client Software Zugriff auf einen E-Mail Server zum Versand von E-Mails an den MPS Server ermöglicht werden.

Die MPS Client Software erstellt keine Auswertungen über die von ihr erfassten Informationen der überwachten Drucksysteme, diese werden alleine von der MPS Server Software bereitgestellt. Außer den von den Drucksystem erfassten Informationen über Zählerstände, Level der Verbrauchsmaterialien, Fehlertstati, Seriennummern, Firmwareständen, etc. und dem in der Konfiguration der MPS Software hinterlegten Kundennamen, werden keine Daten an die MPS Server Software weitergegeben.

4 Überblick über erfasste Daten und Informationen

Vom MPS 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 Stati weiterer Verbrauchsmaterialien, falls vom Gerät gemeldet
- Alarm- und Fehlerzustände 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 MPS Software erfasst und verarbeitet.

Welche Alarm- und Fehlerzustände der Druck- und MFP Systeme von der MPS Client Software erfasst und von der MPS 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 MPS Client Software werden in gerätespezifischen Steuerdateien (PMD Dateien) hinterlegt. Für jeden Gerätetyp existiert eine solche PMD Datei, die der MPS Client Software mitteilt, an welcher Stelle der MIB die erwünschten Informationen über Zählerstände, Level der Verbrauchsmaterialien, etc. beim jeweiligen System per SNMPv2 auszulesen sind. Das Installationspaket der MPS 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 MPS Client Software bzgl. dieser PMD Dateien immer aktuell zu halten, kann innerhalb der MPS Client Software ein tägliches automatisches Update dieser PMD Dateien konfiguriert werden. Ist diese Option eingestellt, so stellt die MPS Client Software einmal täglich zum konfigurierten Zeitpunkt automatisch eine Internet Verbindung zu einem Server der docuFORM GmbH her und lädt von dort ein ZIP Archiv mit den aktuellen PMD Dateien herunter. Dieses Paket wird anschließend automatisch entpackt und in die MPS 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 MPS 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 MPS 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 Passwortgeschützer Zugriff auf die MPS Software

Der Zugriff auf die MPS Client und MPS Server Software erfolgt passwortgeschützt. In der Browser-basierten Weboberfläche der MPS Server Software existieren verschiedene Zugangslevel für Administratoren, Händler und Kunden. Je nach Zugangslevel werden

dem Anwender die dem Zugangslevel entsprechenden Rechte in der MPS Software eingeräumt. Zusätzlich können über sogenannte Zugangscodes zu bestehenden Händler- und Kundenzugängen parallel weitere Händler- und Kundenzugänge mit konfigurierbaren, einschränkbaren Rechten eingerichtet werden.

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

9 MPS Software Prüf- und –freigabeprozess

Jede größere und kleinere Softwarefreigabe durchläuft einen Qualitätssicherungsprozess, in dem mehrere docuFORM Mitarbeiter 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 docuFORM Servern mit Testdaten parallel zu alten Systemen betrieben wird.

10 MPS Quellcodeschutz

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