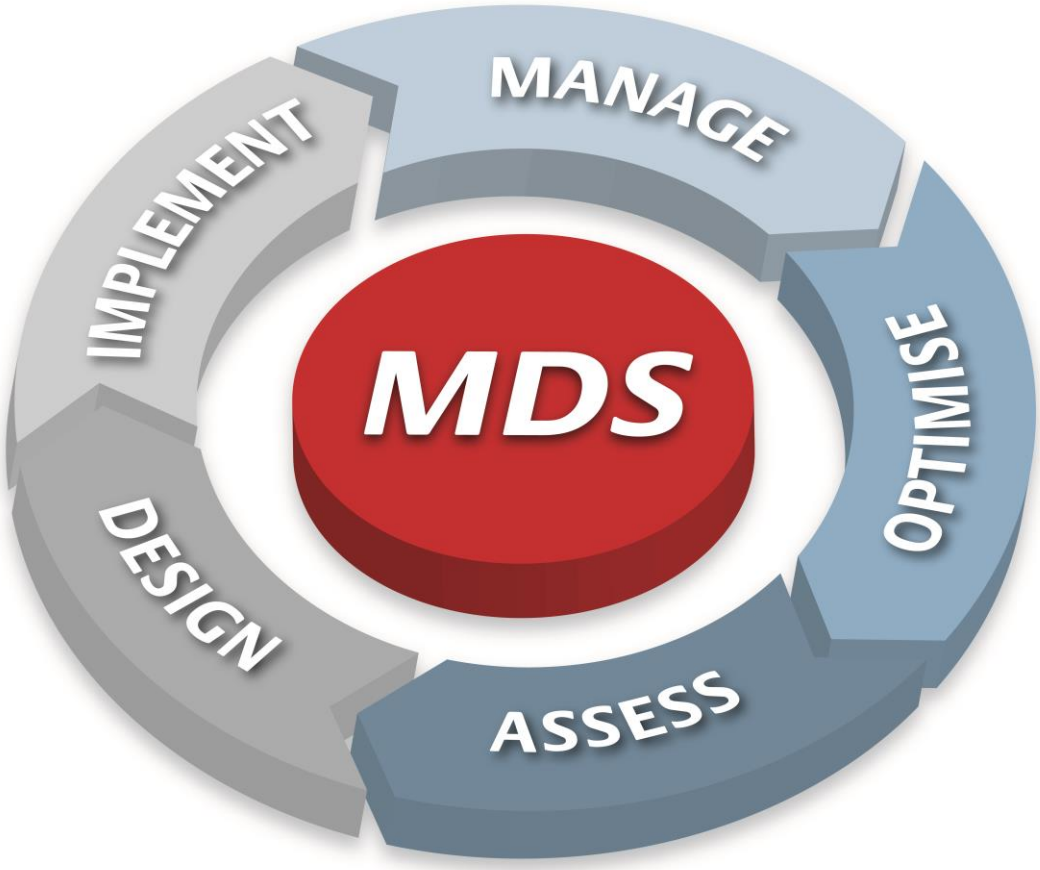
KYOFLEETMANAGER V3 - DATENSICHERHEIT



Managed Document Services (MDS)

- Flottenmanagement

KYOCERA
Document Solutions

Inhaltsverzeichnis

1. ALLGEMEINES

KYOCERA Document Solutions verpflichtet sich, nur Softwareprodukte zur Verfügung zu stellen, die in allen Netzwerkumgebungen sicher verwendet werden können. KYOCERA Softwareprodukte erfassen nur die Daten von bildgebenden Systemen, die für die Verwaltung einer Druckumgebung notwendig sind, es werden keine persönlichen Daten oder Nutzerinformationen gesammelt.

Dieses Dokument befasst sich mit der Netzwerk- und Informationssicherheit bezogen auf:

- KYOfleetmanager Hosted Environment
- KYOfleetmanager Data Collector Agent (DCA)
- KYOfleetmanager Web Console

Weiterhin ist beschrieben, dass bei Verwendung der KYOfleetmanager Software-Anwendungen die Einhaltung folgender Gesetze gewährleistet ist:

- DIN ISO/IEC 27001
- Health Insurance Portability & Accountability Act (HIPAA)
- Sarbanes-Oxley
- Gramm-Leach-Bliley Act (GLBA)
- Federal Information Security Management Act (FISMA)

2. DATENVERWALTUNG

Der gehostete Server befinden sich in einem europäischen Rechenzentrum, welches nach ISO 27001 zertifiziert ist und folgende Sicherheitsvorkehrungen aufweist:

- Datenverarbeitung nach europäischen Datenschutz-bestimmungen
- Redundante, auf Computer optimierte Klima-Kontrollsysteme
- Löschsystem für Gasbrände und präventive Sprinkleranlagen
- Biometrische Zugangskontrolle und Videoüberwachungssystem mit 24-Stunden-/7-Tage-Vor-Ort-Sicherheitspersonal

Zur Vermeidung von Ausfallzeiten und Datenverlust verfügen die gehosteten Server über folgende Sicherheitsfunktionen:

- Redundante glasfaserbasierte Backbone-Anbindung an mehrere Tier 1 Internet Backbone Anbieter
- Vollständige UPS mittels Batterie und Diesel-Notstromaggregat mit Betankungsmöglichkeit im laufenden Betrieb
- Automatisierte Datensicherung

3. GESETZESKONFORMITÄT

3.1 DIN ISO/IEC 27001

Die Verwendung von KYOfleetmanager Software-Anwendungen verstößt nicht gegen die Bestimmungen gemäß DIN ISO/IEC 27001 (International Organization for Standardization). DIN ISO/IEC 27001 ist ein weit verbreiteter globaler Sicherheitsstandard, der Sicherheitsanforderungen für Informationsmanagementsysteme beschreibt. Der Standard bietet eine systematische Vorgehensweise zur Verwaltung von Unternehmens- und Kundendaten, die auf regelmäßigen Risikobewertungen basiert. Um die Zertifizierung zu erhalten, muss ein Unternehmen zeigen, dass es über einen systematischen und kontinuierlichen Ansatz für den Umgang mit Informationssicherheitsrisiken verfügt, die die Vertraulichkeit, Integrität und Verfügbarkeit von Unternehmens- und Kundendaten bedrohen.

Weitere Informationen über DIN ISO/IEC 27001 finden Sie unter:
http://www.iso.org/iso/catalogue_detail?csnumber=42103

3.2 HEALTH INSURANCE PORTABILITY & ACCOUNTABILITY ACT (HIPAA)

Die Verwendung von KYOfleetmanager Software-Anwendungen verstößt nicht gegen die Bestimmungen des Health Insurance Portability & Accountability Act (HIPAA).
Die Verwendung KYOfleetmanager Software-Anwendungen hat bezüglich der betroffenen Einrichtungen/Personen keine Auswirkungen auf die Einhaltung von Rechtsvorschriften des Health Insurance Portability & Accountability Act (HIPAA). KYOfleetmanager Software-Anwendungen sammeln, beherbergen oder übertragen keine Informationen über den Inhalt von Druckaufträgen und ermöglichen daher keinen Zugriff auf elektronisch gespeicherte Patientendaten (ePHI), wie sie unter HIPAA definiert sind.

Weitere Informationen über HIPAA finden Sie unter:
http://www.hhs.gov/ocr/hipaa/

3.3 SARBANES-OXLEY

Die Verwendung von KYOfleetmanager Software-Anwendungen verstößt nicht gegen die Bestimmungen des Sarbanes-Oxley.
Die KYOfleetmanager Software ist nicht für die Verwendung als Teil einer Kontrollstruktur vorgesehen, wie sie in „Abschnitt 404: Management Assessment of Internal Controls“ beschrieben ist, aber wird derartige Kontrollstrukturen nicht behindern.
IT-Kontrollstrukturen sind ein wesentlicher Bestandteil für die Erfüllung von Sarbanes-Oxley. Dieses Gesetz beinhaltet unter anderem die persönliche Verantwortlichkeit von Vorständen für Feststellung, Bewertung und Überwachung der Wirksamkeit interner Kontrollmechanismen über die Richtigkeit von Geschäfts- und Finanzberichten. Es gibt bereits IT-Systeme auf dem Markt, die speziell für die Erfüllung dieser Ziele konstruiert sind. KYOfleetmanager Software ist

selbst kein IT-Kontrollsystem, aber behindert den Einsatz derartiger Systeme nicht und verursacht daher bei einem Einsatz dieser Systeme keine Probleme.

Weitere Informationen über Sarbanes-Oxley stehen unter:
http://www.sec.gov/about/laws/soa2002.pdf

3.4 GRAMM-LEACH-BLILEY ACT (GLBA)

Die Verwendung von KYOfleetmanager Software-Anwendungen verstößt nicht gegen die Bestimmungen des Gramm-Leach-Bliley Act (GLBA).
Die Verwendung KYOfleetmanager Software-Anwendungen hat bezüglich der betroffenen Einrichtungen/Personen keine Auswirkungen auf die Einhaltung von Rechtsvorschriften des Gramm-Leach-Bliley Act (GLBA). KYOfleetmanager Software-Anwendungen sammeln, beherbergen oder übertragen keine Informationen über den Inhalt von Druckjobs und ermöglichen daher keinen Zugriff, keine Aufnahme oder Übertragung von personenbezogenen Finanzdaten, auch wenn derartige Informationen gedruckt oder an Drucksysteme gesendet werden, die von KYOfleetmanager Software-Anwendungen überwacht werden.

Weitere Informationen über Gramm-Leach-Bliley Act finden Sie unter:
http://www.ftc.gov/privacy/privacyinitiatives/glbact.html

3.5 FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA)

Die Verwendung von KYOfleetmanager Software-Anwendungen verstößt nicht gegen die Bestimmungen des Federal Information Security Management Act (FISMA).
Die KYOfleetmanager Software-Anwendungen sind nicht für die Verwendung als internes Kontrollsystem im Sinne von FISMA vorgesehen, aber behindern den Einsatz derartiger Systeme nicht.
Die Verwendung KYOfleetmanager Software-Anwendungen hat bezüglich der betroffenen Einrichtungen/Personen keine Auswirkungen auf die Einhaltung von Rechtsvorschriften des Federal Information Security Management Act (FISMA). KYOfleetmanager Software-Anwendungen sammeln, beherbergen oder übertragen keine Informationen über den Inhalt von Druckjobs und ermöglichen daher keinen Zugriff, keine Aufnahme oder Übertragung von sicherheitsrelevanten Informationen, auch wenn derartige Informationen gedruckt oder an Drucksysteme gesendet werden, die von KYOfleetmanager Software-Anwendungen überwacht werden.

Weitere Informationen über Federal Information Security Management Act finden Sie unter:
http://csrc.nist.gov/groups/SMA/fisma/index.html

4. DATA COLLECTOR AGENT SOFTWARE

Der KYOfleetmanager Data Collector Agent (DCA) ist eine Software-Anwendung für nicht-dedizierte Netzwerkserver, mit der am jeweiligen Standort die Daten von bildgebenden Systemen erfasst werden können. Die bildgebenden Systeme müssen eine Netzwerkschnittstelle besitzen und an das Netzwerk angebunden sein (Netzwerkgeräte), damit der DCA sie zur Datenerfassung scannen kann.
Als Windows® Dienst kann der DCA 24 Stunden am Tag an allen 7 Wochentagen ausgeführt werden. Optional kann der DCA auch als geplante Aufgabe ausgeführt werden.

4.1 AKTIVIERUNG UND DCA AUTHENTIFIZIERUNG

KYOfleetmanager DCA muss vor einer Datenübermittlung an den Server auf einem KYOfleetmanager Enterprise Server aktiviert werden. Die DCA-Aktivierung erfolgt von KFM Server Administratoren und beinhaltet:

- Erstellung eines DCA Account auf dem KFM Server
- Die Verbindung einer DCA Installation mit dem DCA Account basiert auf einer eindeutigen PIN
- Ein gemeinsam verwendeter Schlüssel wird erzeugt und dient zum verschlüsselten Datenaustausch zwischen KFM Server und DCA Installation (für DCAs v. 4.0 und höher)

DCA Accounts können über ein Ablaufdatum verfügen, um die Anmeldeinformationen für die Datenübermittlung an den KFM Server automatisch zu sperren; die Anmeldeinformationen können auch vom KFM Server Administrator jederzeit gesperrt werden, indem dieser den DCA deaktiviert. Zum Zeitpunkt des Ablaufdatums oder einer Deaktivierung des DCA wird die Datenübermittlung sofort vom KFM Server zurückgewiesen.

Für DCAs v.4.0 oder höher prüft der KFM Server, ob der übermittelnde DCA einen gültigen Account auf dem Server besitzt, bevor er die Daten akzeptiert. Nur bei einem bestehenden, aktiven DCA Account werden die Daten zur weiteren Verarbeitung in einer Datei auf dem Server gespeichert; ansonsten wird die Datenübermittlung ignoriert und die Daten werden nicht auf dem Server gespeichert.

Für DCAs 3.x werden die übermittelten Daten in einer Datei auf dem KFM Server gespeichert. Die Gültigkeitsprüfung und Statusprüfung des DCA Accounts erfolgt während der Verarbeitung der Datei. Existiert kein übereinstimmender DCA Account, wird standardmäßig ein neuer DCA 3.x Account erstellt, um Upgrades zu ermöglichen.

Der für den verschlüsselten Datenaustausch zwischen KFM Server und DCA gemeinsam verwendete Schlüssel ist in einer Datenbank auf dem KFM Server gespeichert und mit Hilfe von MS Windows Server und MS SQL Server geschützt. Der Administrator von MS Windows Server und MS SQL Server ist für die Implementierung geeigneter Sicherheitsrichtlinien verantwortlich, um einen unbefugten Zugriff auf den gemeinsamen Schlüssel zu verhindern. Weder KYOfleetmanager Optimizer (KFM Server User Interface) noch andere

KYOfleetmanager Komponenten ermöglichen die Herausgabe des gemeinsamen Schlüssels an Anwender.

Für DCAs 4.0 und höher wird während der DCA Installation der gemeinsame Schlüssel lokal, in einem verschlüsselten Speicherbereich, gespeichert. Der Verschlüsselungsalgorithmus verwendet die Hardware-Parameter und Windows® Produkt ID des DCA Hosts; dadurch ist gewährleistet, dass der gemeinsame Schlüssel nur für die DCA Installation verwendet werden kann, für die er während der DCA-Aktivierung gespeichert wurde.

DCA 3.x speichert die Daten in einer unverschlüsselten Datei, aber ab DCA 3.2 wird ein MD Hash-Code angehängt, um die Datenintegrität zu prüfen. Der KFM Server lehnt alle Dateien ab, die die Gültigkeitsprüfung nicht bestehen und kann optional so eingestellt werden, dass Dateien ohne MD Hash-Code generell zurückgewiesen werden (Dateien vor DCA Version 3.2). Nur wenn HTTPS für die Datenübertragung verwendet wird, sind die Dateien immer verschlüsselt.

5. GESAMMELTE INFORMATIONEN

Während eines Netzwerkscans versucht KYOfleetmanager DCA, von den vernetzten Druck-systemen die folgenden Informationen zu erhalten:

- IP-Adresse (kann unterdrückt werden)
- Seriennummer des Tonerbehälters
- Beschreibung des Systems
- Wartungseinheit – Aktueller Level
- Seriennummer
- Wartungszustand anderer nicht toner basierter Komponenten
- Zählerstände
- Inventarnummer
- Monochrom oder Farbe
- Standort
- LCD-Anzeigen
- MAC-Adresse
- Systemstatus
- Hersteller
- Fehlercodes
- Firmware
- Tonerstände
- Verschiedenes (maschinenspezifisch)

Hinweis:
Es werden keine Druckauftrags- oder Benutzerbezogenedaten gesammelt.

5.1 ERFASSUNGS- UND SENDEMETHODEN

Der DCA sendet die erfassten Daten per HTTPS (Port 443 – empfohlen), HTTP (Port 80), FTP (Port 21/Port 20) oder SMTP (Port 25, über E-Mail) an eine zentrale Datenbank. Die folgende Tabelle beschreibt die bei unterschiedlichen DCA-Versionen verwendeten Protokolle:

DCA	HTTPS-empfohlen	HTTP	FTP	SMTP
DCA v 3.x	Ja	Ja	Ja	Ja
DCA v 4.0	Ja	Ja	Nicht verfügbar	Nicht verfügbar

Die Datenübertragung mit HTTPS ist empfehlenswert, da dieses Protokoll während der Übertragung eine SSL 128-Bit Datenverschlüsselung zur Verfügung stellt. HTTP, FTP und SNMP bieten diese Verschlüsselung nicht. Um mit HTTPS zu übertragen, muss auf der Maschine, die die gesendeten Daten empfängt, ein SSL Sicherheitszertifikat installiert sein.

5.2 SENDEFORMATE

DCAs v.4.0 und höher verschlüsseln die zu übermittelnden Daten mit 128-bit TripleDES unter Verwendung des gemeinsamen Schlüssels sowie der DCA Host Hardware-Parameter und der MS Windows Produkt ID. Dies erhöht den Datenschutz während der Übertragung vom DCA zum KFM Server und bietet zusätzlich die Server-Überprüfung während der DCA Übermittlung. Durch diese zusätzliche Verschlüsselung ist gewährleistet, dass auch bei Nichtbenutzung von SSL (HTTPS) und selbst bei unverschlüsseltem Header/Wrapper der tatsächliche Dateninhalt verschlüsselt ist. SSL (HTTPS) bietet eine zusätzliche Stufe der Sicherheit, da selbst die Message Wrapper verschlüsselt sind. KYOfleetmanager Software verwendet die im Microsoft .Net Framework eingebundenen Verschlüsselungs-Provider, um den Datenaustausch zwischen DCA 4.0 und KFM Server zu verschlüsseln.
DCA 3.x sendet die Daten als kommagetrennte Dateien im einfachen Textformat. Daher wird aus Datenschutzgründen dringend empfohlen, das Übertragungsprotokoll HTTPS zu verwenden.

5.3 NETZWERKVERKEHR

Der von DCA verursachte Netzwerkverkehr ist minimal und variiert abhängig von der Anzahl der zu scannenden IP-Adressen. Die unten stehende Tabelle vergleicht die von DCA verursachte Netzwerklast mit der Netzwerklast, die durch das Laden einer Standard-Webseite entsteht.

Ereignis	Ca. Bytes total
Laden einer Standard-Webseite	60 KB
DCA Scan, einzelne leere IP-Adresse	5,2 KB
DCA Scan, nur 1 Drucker	7,2 KB
DCA Scan, 1 Drucker, 254 IPs	96 KB
DCA Scan, 15 Drucker, 254 IPs	125 KB

5.4 ZUSÄTZLICHE FUNKTIONEN VOM DCA

5.4.1 Optionale Remote Updates

Die optionale Remote Update Funktion von DCA steht zur Verfügung, wenn die Optionen Health Check und Intelligent Update aktiviert sind. Health Check prüft regelmäßig, ob der DCA Dienst noch ausgeführt wird und startet ihn gegebenenfalls neu. Intelligent Update ermöglicht die Prüfung auf vorhandene Software Updates und die Änderung der DCA Konfiguration, wenn ein Administrator dies auf dem KYOfleetmanager Server angewiesen hat. Diese Funktionen sind am Endbenutzerstandort einstellbar und normalerweise nicht notwendig.

5.4.2 DCA Semaphore

Mit der DCA Semaphore Funktion können KYOfleetmanager Server Administratoren die auf dem Server aktivierten DCAs über Befehle remote verwalten; die möglichen Befehle sind:

Deactivate	erzwingt die Deaktivierung des jeweiligen DCA
MIB Walk	zwingt den jeweiligen DCA zur Anforderung aller verfügbaren OIDs des Geräts, dessen IP im Befehlsparameter deklariert ist
Redirect	zwingt den jeweiligen DCA, die Dateiübermittlung an den alten KFM Server zu stoppen, die Übermittlung an den im Parameter "ServerUrl" stehenden KFM Server zu starten und - falls der Parameter "DeActivate" auf "True" gesetzt ist - sich selbst auf dem alten KFM Server zu deaktivieren
Update	zwingt den jeweiligen DCA zur Überprüfung auf verfügbare Updates und - sofern diese vorhanden sind - zur automatischen Aktualisierung anhand dieser Updates.
Uninstall	erzwingt die Deinstallation des jeweiligen DCA

Keiner dieser Befehle kann dazu benutzt werden, den Umfang der zu sammelnden Daten zu vergrößern oder andere als die oben beschriebenen Daten zu sammeln. Der verschlüsselte Datenaustausch zwischen DCA 4.0 und KFM Server verwendet den gleichen Algorithmus wie die Datenübermittlung und basiert auf einem eindeutigen gemeinsamen Schlüssel.

6. KYOFLEETMANAGER WEB CONSOLE

Die KYOfleetmanager Web Console ist die Online-Schnittstelle für das KYOfleetmanager System.

6.1 BERECHTIGUNGSBASIERTE BENUTZERVERWALTUNG

Der Zugriff auf die KYOfleetmanager Web Console wird über eine berechtigungsbasierte Benutzerverwaltung kontrolliert. Die Benutzer müssen sich mit einem festgelegten Benutzernamen und Kennwort in KYOfleetmanager anmelden.

6.2 HTTPS ZUGRIFF

Der Zugriff auf die Webseite kann mittels HTTPS erfolgen, sofern auf dem Webserver ein entsprechendes SSL Sicherheitszertifikat installiert ist. Dies gewährleistet eine 128-Bit Verschlüsselung der Daten während der Übertragung über das Internet.

Stand: September 2013
Irrtum und Änderungen vorbehalten.

Verantwortlich für den Inhalt:
KYOCERA Document Solutions Europe B.V.
(Übersetzung KYOCERA Document Solutions Deutschland GmbH)

KYOCERA Document Solutions Europe B.V.
Otto-Hahn-Str. 12
D-40670 Meerbusch
Telefon: +49(0)2159-928-500
Telefax: +49(0)2159-928-599
info@deu.kyocera.com