Sécurité des périphériques Kyocera

Livre blanc version 1.3

25/07/2022

Sommaire

Introduction

Tout périphérique Kyocera est doté d'un système d'exploitation. Un disque dur ou disque SSD peut être installé dans un multifonction ou une imprimante, comme sur un PC.
Dans les environnements bureautiques, les imprimantes traitent différents types de données sensibles. Elles sont exposées à des menaces aussi diverses que complexes, telles que les accès non-autorisés sur une connexion réseau, la copie ou la modification illicite d'informations en transit, ou des fuites de données. Kyocera Document Solutions Inc. (Kyocera dans ce document) apporte à ses clients un choix étendu de fonctions de sécurité intégrées à ses périphériques d'impression.
Nous mettons constamment en place des mesures proactives contre ces menaces, pour que nos clients puissent utiliser les périphériques Kyocera en toute sécurité et sérénité. En outre, Kyocera a obtenu la certification des Critères Communs (ISO15408). Pour l'obtenir, un prestataire indépendant vérifie objectivement si les fonctions de sécurité sont correctement exécutées pour les utilisateurs. Cette vérification s'applique aussi à des processus rigoureux, tels que la conception des produits, la fabrication ou encore la livraison. Les périphériques Kyocera sont conçus pour offrir des capacités et des fonctions de sécurité adaptées aux besoins. Ils seront d'ailleurs certifiés au cours des prochains mois pour leur conformité à la norme IEEE 2600.1. Depuis 2009, cette norme de sécurité internationale couvre les équipements d'impression. La norme Federal Information Processing Standard créée par l'U.S. National Institute of Standards and Technology (NIST), certifiée FIPS 140-2, est installée sur les équipements Kyocera. Par ailleurs, la société Kyocera est certifiée ISO 27001 en reconnaissance de son engagement à respecter les normes les plus strictes en matière de gestion de la sécurité de l'information en entreprise. Nous sommes donc en mesure de garantir nos périphériques contre les intrusions et failles de sécurité.
Pour protéger ses équipements, Kyocera continue de développer des améliorations pour toutes les fonctions de sécurité, adaptées au développement des normes et à l'évolution des technologies.
Ce document explique comment les fonctions de sécurité installées sur nos multifonctions et imprimantes réagissent contre les menaces et nous permettent de gérer la sécurité.

2. Identification, authentification et autorisation

2.1 Identification et authentification

L'identification et l'authentification constituent un processus important pour vérifier si un utilisateur a la permission requise pour accéder à et utiliser un dispositif. L'utilisateur doit saisir ses informations de connexion, telles qu'un nom d'utilisateur et un mot de passe. Le nom d'utilisateur permet d'identifier le demandeur de la connexion. Le mot de passe est un code alphanumérique que seul cet utilisateur doit connaître.
Pour utiliser la fonction d'identification et d'authentification, les utilisateurs doivent enregistrer à l'avance un nom d'utilisateur et un mot de passe de connexion sur le ou les multifonctions. Par conséquent, seuls les utilisateurs dûment enregistrés sont autorisés à accéder aux périphériques.
Les périphériques Kyocera permettent à un administrateur de gérer les autorisations de manière à attribuer un niveau d'autorisation spécifique à chaque utilisateur, tel que «utilisateur» ou «administrateur». Des fonctions spécifiques peuvent être restreintes ou non pour chaque utilisateur.
Pour accéder à un périphérique, un utilisateur doit être correctement authentifié en saisissant un nom d'utilisateur et un mot de passe valides, afin de protéger les dispositifs contre toute utilisation non-autorisée.
Des journaux des accès permettent de suivre les opérations exécutées sur les périphériques et leurs utilisateurs.

2.1.1 Authentification d'un utilisateur

Cette fonction protège les informations en contrôlant les accès et l'identification des utilisateurs autorisés sur les périphériques.
Cette fonction supporte donc le contrôle des accès et la protection des ressources.
Lorsque le nom d'utilisateur et le mot de passe saisis correspondent aux données préenregistrées, l'utilisateur est authentifié et autorisé à accéder aux périphériques.

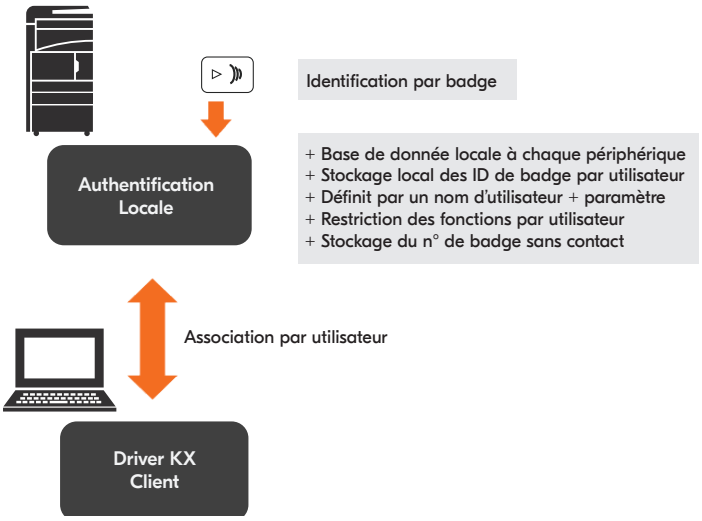
Politique de mot de passe
La politique de mot de passe encourage les utilisateurs à choisir des mots de passe forts, basés sur divers paramètres, tels que longueur minimale, complexité, durée de validité. La fonction rejette les mots de passe qui ne sont pas conformes à cette politique. Elle évite donc les mots de passe faibles définis par des utilisateurs.
Politique de blocage de compte
La fonction de blocage de compte verrouille temporairement le compte lorsque le nombre maximal de tentatives d'accès est atteint dans un délai prédéterminé. Le nombre de tentatives (de 1 à 10) avant verrouillage et la durée de ce verrouillage (de 1 à 60 minutes) peuvent être défini. Le compte utilisateur est bloqué lorsque le nombre maximal de tentatives d'accès avec un mot de passe erroné est atteint. La configuration de la politique de blocage de compte contribue largement à minimiser les risques posés par les stratégies de résolution de mot de passe ciblant des périphériques (telles que les attaques par force brute).

2.1.2 Mode d'Authentification

Les périphériques Kyocera offrent les modes d'authentification suivants.

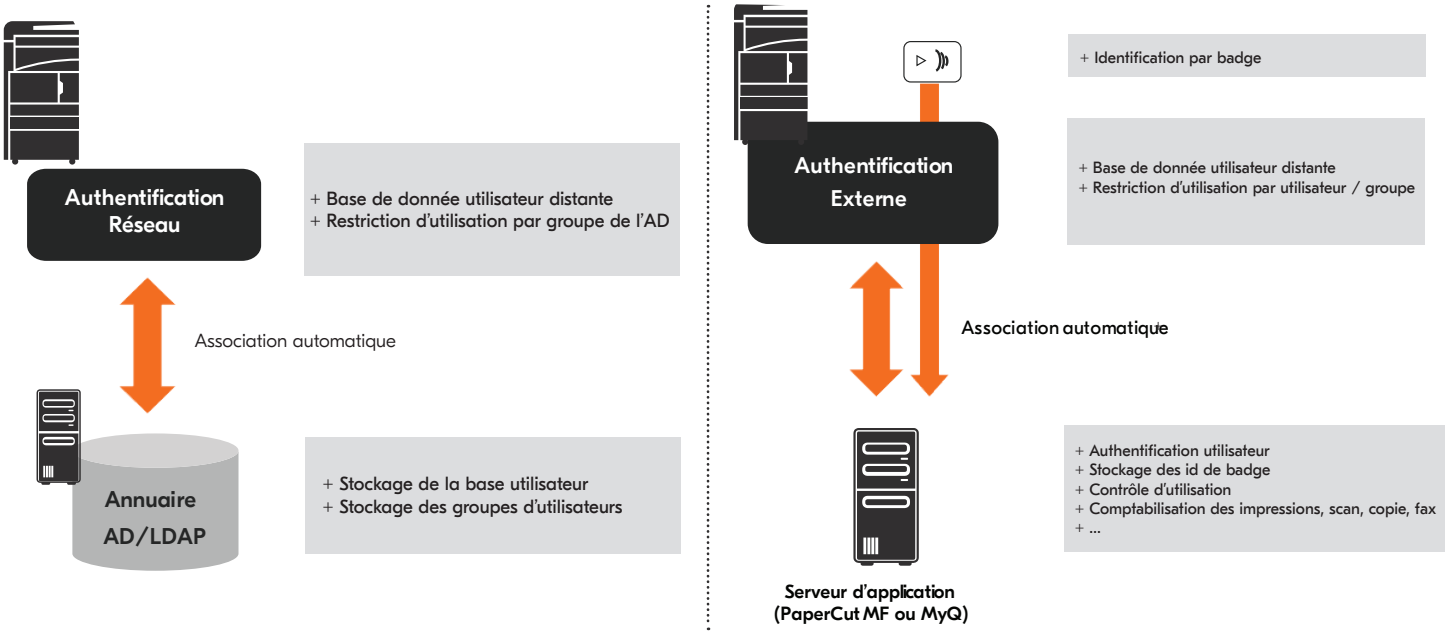
Authentification Locale

Le mode Authentification locale authentifie les utilisateurs en fonction des données enregistrées dans la liste des utilisateurs locaux sur les périphériques. Seuls les utilisateurs enregistrés peuvent accéder aux périphériques.



Authentification Réseau

Le mode Authentification Réseau authentifie les utilisateurs grâce à un serveur d'authentification. Les utilisateurs peuvent accéder aux dispositifs grâce aux données des utilisateurs enregistrées sur le serveur d'authentification. Des serveurs tels que les NTLM et Kerberos sont disponibles, ainsi que les flux avec des serveurs tiers.



Authentification Kerberos

Kerberos authentifie les utilisateurs entre un client et un serveur d'authentification sur un réseau. Ce système unifie plusieurs serveurs et des données d'authentification d'utilisateur. Il permet aux utilisateurs de bénéficier des avantages d'une connexion unique. Des canaux de communication peuvent être chiffrés.

Authentification NTLM

L'authentification NTLM supporte les accès réseau nécessaires aux connexions des périphériques sur le réseau. NTLM interpose un mode d'interrogation-vérification entre des périphériques et un serveur pour éviter la transmission de mots de passe non-cryptés sur le réseau. Les données d'interrogation émises par le serveur sont cryptées. Le hash NTLM fonctionne comme clé de chiffrement.

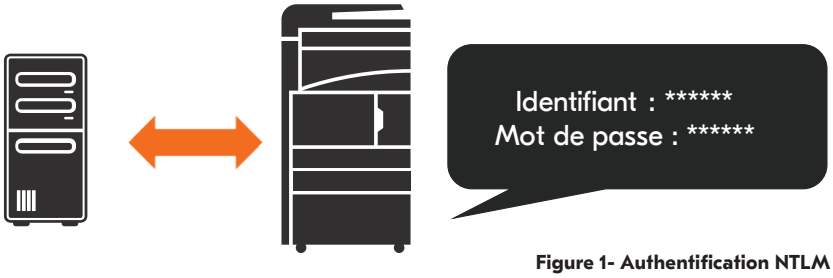


Figure 1- Authentification NTLM

2.1.3 Connexion des périphériques

Les modes de connexion suivants peuvent aussi être utilisés à la place de la saisie d'un nom d'utilisateur et d'un mot de passe sur un panneau de contrôle.

Authentification par badge (Option)

L'authentification par cartes d'identification supporte deux approches. L'une consiste à se connecter avec seulement une carte d'identification et l'autre à présenter une carte d'identification devant un lecteur de cartes puis à entrer un mot de passe. L'authentification par carte d'identification peut être utilisée en mode d'authentification locale. (Figure 2)

Lorsqu'une carte d'identification a été préalablement enregistrée dans la liste des utilisateurs sur des multifonctions / imprimantes, ou dans un serveur d'authentification externe ou tiers, l'utilisateur est autorisé à accéder aux dispositifs avec sa carte d'identification.
L'authentification avec une carte d'identification, telle qu'une carte d'employé ou un badge d'accès, permet d'utiliser les fonctions de gestion des services et des utilisateurs. Des fonctions spécifiques peuvent être restreintes en fonction des données d'utilisateur associées aux cartes d'identification. (Figure 3)

Figure 2 - Authentification par badge

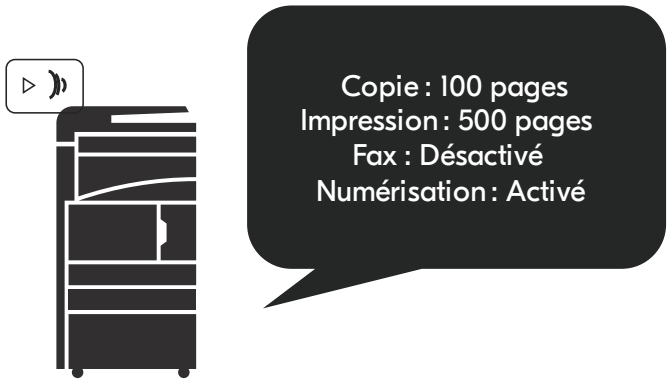


Figure 3 – Restriction de fonction avec authentification locale

2.2 Autorisation

L'utilisation de fonctions spécifiques, telles que l'impression couleur, la copie couleur, la télécopie, les boîtes de stockage ou encore l'utilisation de mémoires de stockage externes, peut être restreinte par les utilisateurs autorisés. Cette fonction contribue largement à réduire les possibilités de fuites d'informations sur des périphériques. Selon les différents niveaux d'autorisation («utilisateur, «administrateur» ou «administrateur de dispositif»), l'accès aux paramètres des périphériques peut aussi être contrôlé. Certains périphériques offrent la possibilité de restreindre des fonctions telles combiner, le recto-verso ou le mode EcoPrint. Par exemple, un utilisateur qui n'est pas autorisé à sélectionner «ne pas combiner» doit choisir «2 en 1» ou plus, pour faire des copies.

2.2.1 Mode Autorisation

Les périphériques Kyocera offrent les modes d'autorisation suivants.

Autorisation Locale
La fonction Autorisation Locale permet d'utiliser une liste d'utilisateurs locaux enregistrés sur un multifonction pour supporter l'authentification locale. L'utilisation peut être définie pour chaque utilisateur.

Autorisation Réseau (Autorisation de groupe)
La fonction Autorisation Réseau utilise des informations de groupe obtenues par authentification de réseau ainsi que des données d'autorisation préalablement stockées sur les multifonctions. Des restrictions peuvent être appliquées en fonction des groupes enregistrés sur le serveur d'authentification. L'utilisation des multifonctions peut être restreinte pour le groupe enregistré sur le serveur, renforçant ainsi la sécurité des dispositifs utilisés par ce groupe.

Connexion par fonction (avec ou sans compte invité)
La connexion est restreinte par des fonctions : Restriction d'impression, Restriction d'impression en couleur, Restriction de copie, Restriction de copie en couleur, Restriction EcoPrint lorsque l'autorisation invité est activée. Les utilisateurs souhaitant utiliser les fonctions avec des restrictions de connexion doivent être authentifiés. Par conséquent, un nombre limité d'utilisateurs préalablement enregistrés sur la liste peuvent utiliser les fonctions spécifiées. Cette fonction de sécurité peut efficacement prévenir les fuites d'informations sur des périphériques Kyocera tout en maintenant la facilité d'utilisation.

2.2.2 Gestion des autorisations des utilisateurs

Concernant la gestion des autorisations des utilisateurs, les fonctions sont uniquement accessibles en fonction des différents niveaux d'autorisation attribués aux utilisateurs.
Les autorisations des utilisateurs incluent : Administrateur machine (device Admin), Administrateur (Admin) et Utilisateur (User). Par conséquent, les utilisateurs non-autorisés ne peuvent pas utiliser la fonction spécifiée.

2.3 Administration des sessions de connexions

La fonction Administration des sessions permet de gérer la durée des sessions de connexions définie par l'heure de l'accès d'un utilisateur à un multifonction et l'heure de sa déconnexion, après authentification.
Seule la fonction d'administration suivante est actuellement disponible :
Réinitialisation automatique du panneau
La fonction Réinitialisation automatique du panneau de commande permet de déconnecter automatiquement ce panneau, de réinitialiser ses paramètres et de rétablir ses valeurs par défaut lorsqu'aucune opération n'a été effectuée après un certain délai. Les utilisateurs peuvent programmer le délai de réinitialisation après la dernière opération. La fonction Réinitialisation automatique du panneau protège les multifonctions contre les accès non-autorisés et les attaques malveillantes lorsque le dernier utilisateur ne s'est pas correctement déconnecté du système.

3. Sécurité du réseau

3.1 Définir le niveau de sécurité du réseau

Les périphériques Kyocera peuvent limiter leurs communications sur le réseau en utilisant simplement une gamme d'adresses IP et de numéros de ports. Le puissant algorithme de hachage sécurisé est également disponible pour les certificats de serveur TLS. Cet algorithme empêche l'altération des données, l'écoute des données et l'usurpation d'identité sur un réseau. En utilisant la fonction de configuration rapide de la sécurité, un administrateur peut sélectionner un niveau approprié parmi les niveaux 1, 2 et 3 en fonction de sa politique de sécurité. Il est possible d'exécuter plusieurs fonctions de sécurité, telles que le paramétrage du réseau, le paramétrage du verrouillage d'interface et le paramétrage du journal, de manière collective et en une seule fois, en fonction du niveau sélectionné. Les utilisateurs peuvent utiliser les périphériques Kyocera en toute sécurité dans l'environnement le plus approprié, conformément à leur politique de sécurité.

3.1.1 Paramétrage du filtrage IP

La fonction Filtrage IP permet de contrôler les accès réseau aux périphériques en définissant des plages d'adresses IP ou des protocoles réseaux à autoriser ou à refuser.

Le filtrage autorise seulement les accès aux clients dont l'adresse IP est enregistrée dans la plage ou les plages d'IP configurées. Certains protocoles peuvent être sélectionnés afin d'être activés ou désactivés.
Pour le support des protocoles IPv4 et IPv6, il est possible de configurer des communications depuis un seul hôte réseau (adresse unique ou multiple) ou des communications depuis plusieurs hôtes réseaux (plages d'IP), ainsi que les protocoles activés pour chacun d'entre eux tels que :

- IPP / IPPS (protocole d'impression réseau)
- HTTP / HTTPS (protocole de transmission de données entre un serveur Web et navigateur Web).
- Raw (protocole d'impression réseau)

Par extension, tout protocole non autorisé est interdit, permettant de sécuriser les périphériques.

3.1.2 Paramétrage des protocoles réseaux

Le paramétrage réseaux permet d'activer ou désactiver des protocoles utilisés sur les périphériques. La désactivation d'un protocole entraine l'arrêt de l'écoute du ou des ports UDP/TCP associés.

Protocole	N°. de port	Configuration	Remarque
Serveur FTP	TCP 21	Activer/ Désactiver	Le protocole FTP est utilisé pour la réception de documents via le protocole FTP
HTTP	TCP 80	Activer/ Désactiver	Le protocole HTTP sert à envoyer / recevoir des données à partir d'une page Web entre un serveur et un navigateur.
NetBEUI	TCP 139	Activer/ Désactiver	Le protocole NetBEUI sert à partager des fichiers et des services d'impression, et pour recevoir des documents sur des réseaux de petites tailles.
HTTPS	TCP 443	Activer/ Désactiver	Le protocole HTTPS supporte le chiffrement des données grâce à SSL/TLS.
IPP over TLS	TCP 443	Activer/ Désactiver	Le protocole IPP over TLS (IPPS) combine le protocole TLS, qui chiffre un canal, et le protocole IPP utilisé pour l'impression par IP. En outre, IPP over TLS accepte les certificats électroniques.
LPD	TCP 515	Activer/ Désactiver	Le protocole d'impression LPD sert à imprimer des fichiers textes ou Postscript.
IPP	TCP 631	Activer/ Désactiver	Le protocole IPP contrôle les envois et réceptions de données d'impression via TCP/IP. Il a été conçu pour l'impression via le réseau Internet.
Thin Print	TCP 4000	Activer/ Désactiver	Thin Print est une technologie d'impression disponible dans un environnement Thin client. Il supporte également SSL.
WSD Scan	TCP 5358	Activer/ Désactiver	Le protocole WSD permet à un hôte d'établir une connexion réseau avec un périphérique scanner de documents. Il permet aux utilisateurs de détecter, d'installer et d'utiliser simplement des périphériques de scan. L'image d'un document numérisé par un multifonction peut être stockée comme fichier sur un PC via le protocole WSD.
WSD Print	TCP 5358	Activer/ Désactiver	Le protocole WSD permet à un hôte d'établir une connexion réseau avec un périphérique d'impression. Il permet aux utilisateurs de détecter d'installer et d'utiliser simplement des périphériques d'impression.
Enhanced WSD	TCP 9090	Activer/ Désactiver	Enhanced WSD (Web Services) offre la possibilité aux outils d'administration Kyocera de se connecter aux périphériques à des fins d'administrations et de gestions.
Enhanced WSD over TLS	TCP 9091	Activer/ Désactiver	Le protocole Enhanced WSD (TLS) combine les protocoles Enhanced WSD et TLS. Il supporte le chiffrement, l'authentification et la protection contre les modifications sur le réseau.
RAW	TCP 9100-9103	Activer/ Désactiver	Pour l'impression, le protocole RAW inclut des étapes différentes de celles du protocole d'impression LPR. En général, les périphériques utilisent le port 9100 et SNMP pour configurer et contrôler l'état des imprimantes.
SNMPv1/v2	UDP161	Activer/ Désactiver	Le protocole SNMP est utilisé par les administrateurs réseau afin de superviser et de paramétrer les équipements connectés au réseau.
SNMPv3	UDP161	Activer/ Désactiver	Le protocole SNMPv3 est une extension de SNMv1/V2 permettant d'inclure des fonctions de sécurisation, telles que le chiffrement des communications et l'authentification par nom d'utilisateur et mot de passe.
DSM Scan		Activer/ Désactiver	DSM (Distributed Scan Management) sur Windows Server 2008 R2 permet de gérer d'importants volumes de données scannées nécessaires dans certaines grandes organisations.
Client FTP		Activer/ Désactiver	Le protocole de communication client FTP sert à transférer des fichiers sur un réseau depuis le périphérique de scan.
LDAP		Activer/ Désactiver	Le protocole LDAP permet aux périphériques de récupérer depuis l'annuaire d'entreprise des informations telles que les courriels et les numéros de fax.
POP3		Activer/ Désactiver	Le protocole POP3 sert à recevoir des e-mails.
POP3 over TLS		Activer/ Désactiver	Le protocole POP3 over TLS combine POP3 (et TLS pour le chiffrement des canaux de communication)
SMTP		Activer/ Désactiver	Le protocole SMTP sert à envoyer des e-mails.
SMTP over TLS		Activer/ Désactiver	Le protocole SMTP over TLS combine SMTP (envoi d'e-mails) et TLS pour le chiffrement des canaux de communication)
SMB Client		Activer/ Désactiver	Le protocole SMB permet le partage de fichiers ou d'imprimantes sur un réseau.

Protocole	N°. de port	Configuration	Remarque
eSCL		Activer/ Désactiver	Le protocole eSCL est un protocole de numérisation pour MAS OS X.
eSCL over TLS		Activer/ Désactiver	Le protocole eSCL over TLS est un protocole de communication eSCL utilisant un certificat TLS pour chiffrer les communications.
LLTD		Activer/ Désactiver	LLTD est un protocole de découverte de la topologie du réseau et de diagnostic de la qualité de service.
Privet		Activer/ Désactiver	Privet est un protocole qui permet de découvrir les appareils connectés au Cloud sur le réseau local et fournit des interfaces pour obtenir des informations sur l'appareil et effectuer certaines actions, telles qu'envoyer un travail d'impression en local.
DNS over TLS	TCP 853	Activer/ Désactiver	DNS over TLS est un protocole qui chiffre les requêtes et les réponses DNS à l'aide de TLS.
SCEP		Activer/ Désactiver	Le protocole SCEP (Simple Certificate Enrollment Protocol) est un protocole qui émet automatiquement un certificat vers les périphériques concernés.
OCSP / CRL		Activer/ Désactiver	La liste de révocation de certificats (CRL) est une liste qui fournit un numéro de série du certificat qui a été révoqué par l'Autorité de Certification. Online Certificate Status Protocol (OCSP) est un protocole qui permet aux navigateurs Web et à d'autres clients d'interroger l'état d'un certificat individuel en temps réel.
REST		Activer/ Désactiver	REST (representational state transfer) est un style d'architecture logicielle définissant un ensemble de contraintes à utiliser pour créer des services Web. Les services web conformes au style d'architecture REST établissent une interopérabilité entre les ordinateurs sur Internet.
REST over TLS		Activer/ Désactiver	REST over TLS est une communication de type REST utilisant un certificat TLS. Toutes les communications REST sur TLS sont chiffrées.
Bonjour		Activer/ Désactiver	Bonjour est une technologie de réseau qui permet aux utilisateurs de découvrir automatiquement les appareils.
VNC		Activer/ Désactiver	Virtual Network Computing (VNC) est un logiciel de contrôle à distance qui utilise le protocole RFB pour accéder à l'interface graphique d'un dispositif à distance par l'intermédiaire d'une connexion réseau.
VNC over TLS		Activer/ Désactiver	VNC over TLS est un logiciel de contrôle à distance qui utilise le protocole RFB pour contrôler l'interface graphique d'un périphérique distant à partir d'une connexion réseau entre un ordinateur (administrateur uniquement) et un périphérique via TLS et ce grâce à un mot de passe unique (OTP — One Time Password).

3.2 Protocole d'authentification réseau

Les périphériques Kyocera supportent l'authentification réseau IEEE 802.1x.
Les protocoles SMTP, POPS, POP before SMTP permettent également de sécuriser, fiabiliser et sécuriser l'authentification.
Les protocoles d'authentification sont généralement intégrés aux protocoles dits de protections de canaux de communication (voir chapitre suivant).

3.2.1 IEEE802.1X

IEEE802.1x est un protocole permettant le contrôle d'accès aux équipements connectés à un réseau.
Il a été mis au point par l'IEEE (Institute of Electrical and Electronics Engineers).
Il permet d'autoriser uniquement les périphériques réseaux préalablement authentifiés à avoir accès aux réseaux.
Il interdit donc la connexion au réseau de périphériques non habilités.
Les périphériques Kyocera offrent 4 modes de fonctionnements :

- **Protocoles PEAP-TLS/PEAP**

Protected Extensible Authentication Protocol-Transport Layer Security
Le client est simultanément authentifié par son identifiant, son certificat et le serveur d'authentification.

- **Protocoles EAP-PEAP**

Extensible Authentication Protocol-Protocol Extensible Authentication Protocol
Le client est simultanément authentifié par son identifiant / mot de passe et le nom commun du certificat sur le serveur d'authentification.

- **Protocoles EAP-FAST**

Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling
EAP-FAST est une méthode d'authentification IEEE802.1. x/EAP développée par Cisco System, Inc. L'authentification mutuelle entre le client et le serveur d'authentification est réalisé grâce à des identifiants et mots de passe. Le PAC (Protected Access Credential) crée un tunnel virtuel pour l'utilisateur avec une clé secrète partagée et unique.

- **Protocoles EAP-TTLS**

Extensible Authentication Protocol-Tunneled Transport Layer Security
Le client est simultanément authentifié par son identifiant / mot de passe et le certificat électronique sur le serveur d'authentification.
Comme pour EAP-TLS, les certificats électroniques Client et Serveur sont exigés par le processus d'authentification, alors que pour EAP-TTLS, l'identifiant / mot de passe remplacent le certificat client. EAP-TTLS est donc plus facile à mettre en œuvre qu'EAP-TLS. Les certificats électroniques permettent de valider mutuellement l'identité du serveur d'authentification et du client. Cette solution améliore la sécurité des communications

3.2.2 Authentification SMTP

La fonction Authentification SMTP permet d'envoyer uniquement un courriel lorsqu'une authentification préalable par identifiant et mot de passe a été correctement réalisée sur le serveur SMTP. Elle contrôle l'accès au serveur SMTP et empêche des périphériques ou utilisateurs non-authaurisés d'envoyer des courriels sur ce serveur.

3.2.3 POP before SMTP

Le protocole POP before SMTP effectue une authentification POP avant d'autoriser le serveur SMTP à envoyer des e-mails. Ce mode de fonctionnement permet de s'assurer que le client s'authentifiant par le protocole POP, utilise la même adresse IP que pour l'émission de son courriel en SMTP et empêche le masquage d'adresses IP (masquerading).

3.3 Protection des canaux de communication

Cette protection sécurise les canaux de communication du réseau. Selon les objectifs et les programmes de chiffrement, divers protocoles sont disponibles. Les périphériques Kyocera supportent les protocoles indiqués ci-dessous pour protéger efficacement les données contre les modifications et les fuites sur le réseau (intégrité et authenticité des échanges).

3.3.1 SNMPv3

Le protocole standard SNMP surveille et contrôle les dispositifs connectés au réseau. SNMPv3 permet de protéger la confidentialité des données grâce à l'authentification et au chiffrement.

3.3.2 IPv6

IPv6 vient remplacer à terme le protocole IPv4. Les périphériques Kyocera sont compatible IPv6s (IPv6 Ready Phase 2).
Le support IPv6 permet de se connecter aux réseaux compatibles et utilise diverses fonctions de contrôle et de gestion telles que l'attribution automatique d'adresses IP et la renumérotation des mécanismes de sécurité comme IPSEC.

3.3.3 IPSec

Le protocole IPSec offre une fonction qui protège les données en transit contre les risques d'accès ou de modification, grâce à un chiffrement des paquets IP. Pour envoyer ou recevoir des données en utilisant IPSec, les périphériques et les hôtes configurés avec IPSec se connectent au réseau avant d'être configurés par les fonctions programmées IPSec. Le chiffrement IPSec protège les données d'impression envoyées par un hôte à un périphérique, ainsi que les données numérisées envoyées par un multifonction à un PC. IPSec renforce donc la sécurité des données.

3.3.4 TLS

Le système TLS sert à chiffrer les données transmises sur des accès Web ou autres protocoles réseaux. Il intègre une fonction de vérification d'identification des hôtes. Les périphériques Kyocera supportent les protocoles de chiffrement TLS, tels que SSL3.0, TLS1.0, TLS1.1, TLS1.**2, TLS 1.3,** pour interdire les accès et les modifications de données échangées sur le réseau. Nous préconisons l'usage des dernières versions de TLS (TLS 1.3) et la désactivation des anciennes verisons (SSL3.0, TLS 1.0, TLS 1.1 à minima).

En outre, le puissant algorithme de hachage sécurisé peut être utilisé pour la communication entre unserveut et un client TLS afin de sécuriser les protocoles suivants :

IPP over TLS
Le protocole d'impression Internet IPP over TLS combine IPP (échange de données d'impression sur Internet ou un réseau TCP/IP) et TLS (chiffrement du canal de communication). Il permet aux utilisateurs d'envoyer des commandes d'impression sécurisées aux périphériques sur le réseau.

HTTP over TLS
HTTP over TLS est un protocole qui combine HTTP (envoi / réception de données entre navigateurs et autres dispositifs sur un réseau TCP/IP) et TLS (chiffrement du canal de communication). Pour la transmission de données entre les PC et périphériques, cette solution réduit les risques de modification et de fuites de données générées par des utilisateurs non-autorisés.

FTP over TLS
Le protocole FTP over TLS combine FTP (transfert de fichiers sur un réseau TCP/IP) et TLS (chiffrement du canal de communication). Le chiffrement TLS est appliqué sur le canal qui transmet des données numérisées provenant d'un périphérique qui utilise le protocole FTP. FTP over TLS renforce la sécurité des transmissions.

Thin Print over TLS (Option)
Thin Print over TLS est un protocole qui combine Thin Print (contrôle de bande passante et compression des tâches d'impression) et TLS (chiffrement du canal de communication). Il accélère et sécurise les tâches dans un environnement d'impression.

SMTP over TLS
SMTP over TLS combine la transmission des e-mails et TLS qui assure le chiffrement du canal de communication entre un serveur et un périphérique. Il bloque le masquage d'adresses IP (masquerading), l'accès ou la modification des données en transit. Il intègre également une fonction d'authentification.

POP over TLS
POP over TLS combine la transmission POP (protocole de réception des e-mails) et TLS qui assure le chiffrement du canal de communication entre un serveur et une imprimante. Il bloque le masquage d'adresses IP (masquerading), l'accès ou la modification des données en transit.

3.4 Fonction de restriction d'envoi / reception de courriels

Les périphériques Kyocera permettent les restrictions d'envoi et de réception indiquées ci-dessous et interdit donc la transmission d'e-mails non-autorisés ou des actions malveillantes effectuées par des utilisateurs non-autorisés.

3.4.1 S/MIME

Secure/Multipurpose Internet Mail Extensions (S/MIME) est une technologie qui permet aux utilisateurs de chiffrer et de signer numériquement leurs courriels. Si un certificat d'utilisateur et un certificat intermédiaire ont été importés dans un appareil Kyocera, un message envoyé par l'appareil peut être chiffré avec la clé publique de l'utilisateur. Cela empêche la capture du message en transit par un tiers. De même, si un certificat de périphérique est installé sur un équipement Kyocera, une signature numérique créée avec la clé privée du périphérique peut être jointe. Cela empêche le message d'être usurpé et modifié par un tiers (assurance de l'expéditeur).

3.4.2 Wi-Fi Direct (option)

Les appareils Wi-Fi Direct peuvent se connecter les uns aux autres sans devoir passer par un point d'accès. Autrement dit, vous n'avez pas besoin d'utiliser un routeur. En effet, les appareils Wi-Fi Direct établissent leurs propres réseaux ad hoc au fur et à mesure des besoins. Ces réseaux fonctionnent dans un domaine de sécurité indépendant de tout réseau d'infrastructure. La carte Wi-Fi Direct optionnelle utilise les standards WPS et WPA2-PSK (Personal) pour permettre aux utilisateurs de configurer facilement la connexion. Cela empêche les connexions de périphériques non authentifiés au réseau indépendant fourni par le MFP/imprimante, protégeant ainsi le périphérique contre toute usage non autorisée.

3.4.3 Fonction de restriction des destinations courriels

Les destinations des courriels peuvent être restreintes par une fonction de contrôle des envois supportant l'autorisation ou l'interdiction d'envoi. Les courriels peuvent uniquement être envoyés à des destinations autorisées et préalablement enregistrées (Liste blanche). Les destinations refusées sont également préenregistrées pour éviter d'envoyer des courriels à des adresses non-autorisées (Liste noire).

3.4.4 Fonction de restriction des expéditeurs

Les périphériques Kyocera sont dotés d'une fonction d'impression des pièces jointes aux courriels. La réception des courriels peut être restreinte conformément aux paramètres de la fonction Restriction des expéditeurs. Les adresses des expéditeurs autorisés doivent être préalablement enregistrées pour que seuls soient acceptés des e-mails provenant d'adresses autorisées (Liste blanche). Les adresses des expéditeurs refusés sont également préenregistrées (Liste noire). Ces mesures de sécurité assurent une protection efficace contre diverses activités malveillantes et les courriels indésirables.

3.4.5 Gestion automatisée des certificats

Les utilisateurs peuvent renforcer la sécurité en ajoutant le logiciel KYOCERA ACM (Automated Certificate Management) pour faciliter la gestion d'opérations très complexes. L'ACM comprend des fonctions d'authentification et de chiffrement TLS et peut superviser les validations d'inscription et de réinscription et surveiller les dates d'expiration des certificats en utilisant SCEP (Simple Certificate Enrollment Protocol), OCSP (Online Certificate Status Protocol) et CRL (Certificate Revocation List). L'ACM supprime le problème de sécurité lié à l'utilisation d'un certificat non valide en vérifiant la date d'expiration d'un certificat et en réinscrivant ou en renouvelant les certificats s'ils ont expiré. En outre, le chiffrement 4096 bits disponible pour les certificats assure une protection contre les attaques avancées de certificats et de PKI. L'ACM peut également garantir la conformité avec la politique de sécurité des utilisateurs.

3.4.6 Récupérer un certificat de dispositif émis par une Autorité de Certification à partir d'un serveur de protocole d'inscription de certificat simple.

Une demande d'émission de certificat est envoyée à un serveur SCEP (Simple Certificate Enrollment Protocol) qui gère les certificats de dispositifs, ainsi qu'une CRL (Certificate Revocation List - liste de révocation de certificats) créée sur la base des informations fournies par les administrateurs. Un certificat émis par une autorité de certification et récupéré sur le serveur SCEP est automatiquement enregistré comme certificat de dispositif après vérification. La gestion des certificats émis par l'Autorité de Certifications est simplifiée par ce processus automatisé qui maintient la sécurité. Seuls les utilisateurs disposant de privilèges d'administrateur peuvent sélectionner les paramètres SCEP.

3.4.7 Vérifier l'état de révocation d'un certificat

Il existe deux méthodes pour vérifier l'état de révocation d'un certificat :

1. Envoyer une requête pour un répondeur OCSP (Online Certificate Status Protocol)
2. Comparer le certificat avec la CRL (Certificate Revocation List - liste de révocation de certificats) enregistrée dans un MFP/imprimante.

Ces deux méthodes sont disponibles afin que les utilisateurs soucieux de la sécurité puissent choisir une méthode adaptée à leur environnement.

Seuls les utilisateurs disposant de privilèges d'administrateur peuvent sélectionner OCSP/CRL (vérification des certificats).

3.4.8 Paramètres du niveau de vérification des certificats du serveur par protocole

Le niveau de vérification du certificat d'un serveur peut varier en fonction du serveur de destination dans l'environnement de sécurité d'un utilisateur. Cette fonction permet de régler le niveau de vérification du certificat du serveur de 0 à 3 par protocole (par exemple, SMTP/POP3/FTP/LDAP/DNS). Le niveau de vérification du certificat du serveur peut être défini comme suit : niveau (0) aucune vérification, niveau (1) vérification de la date d'expiration, niveau (2) vérification de la date d'expiration et de la chaîne, niveau (3) vérification de la date d'expiration, de la chaîne et confirmation de la révocation.
Notez que la connexion à un serveur de destination doit être sécurisée par un chiffrement TLS. La destination légitime de la connexion et le certificat autorisé peuvent être confirmés.

Seuls les utilisateurs disposant de privilèges d'administrateur peuvent sélectionner les paramètres.

3.4.9 Paramètres du niveau de vérification du certificat du dispositif

Cette fonction définit les niveaux de vérification du certificat du dispositif (0 à 3). Le niveau de vérification du certificat du périphérique peut être défini comme suit : niveau (0) aucune vérification, niveau (1) vérification de la date d'expiration, niveau (2) vérification de la date d'expiration et de la chaîne, et niveau (3) vérification de la date d'expiration, de la chaîne et de la révocation.

Notez que la connexion à un client doit être sécurisée par un chiffrement TLS. Les certificats de confiance peuvent être conservés dans les MFP/imprimantes.

Seuls les utilisateurs disposant de privilèges d'administrateur peuvent sélectionner les paramètres.

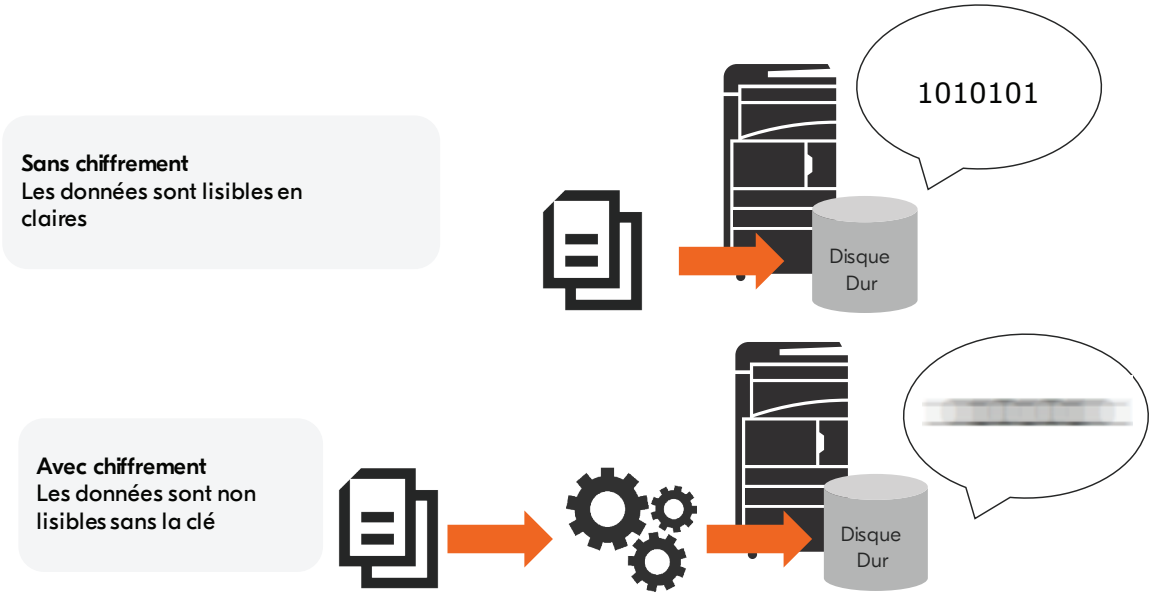
4 Protection des données stockées

4.1 Protection des données

Les informations sensibles ou confidentielles stockées sur des disques durs ou SSD doivent être protégées contre les risques de fuites de données sur des périphériques. Kyocera met en œuvre diverses mesures de protection pour protéger les informations stockées. Elles incluent les fonctions décrites ci-dessous pour garantir que nos clients utilisent les périphériques Kyocera en toute sécurité.

4.1.1 Chiffrement de disques durs / SSD (en standard ou en option selon les modèles)

La fonction de chiffrement des disques durs/SSD permet de chiffrer des documents, des paramètres utilisateurs et des informations du périphérique afin de les stocker sur des disques durs/ SSD des périphériques Kyocera. Le chiffrement utilise les algorithmes AES (Advanced Encryption Standard) 128 bits et 256 bits : FIPS PUB 197. Même si un disque dur ou SSD n'est plus connecté à un périphérique, par exemple emporté par une personne malveillante, les données sensibles ou confidentielles qu'il contient restent protégées et inexploitables



4.1.2 Sécurisation de la clé de chiffrement par module TPM - (Trusted Platform Module) (selon les modèles)

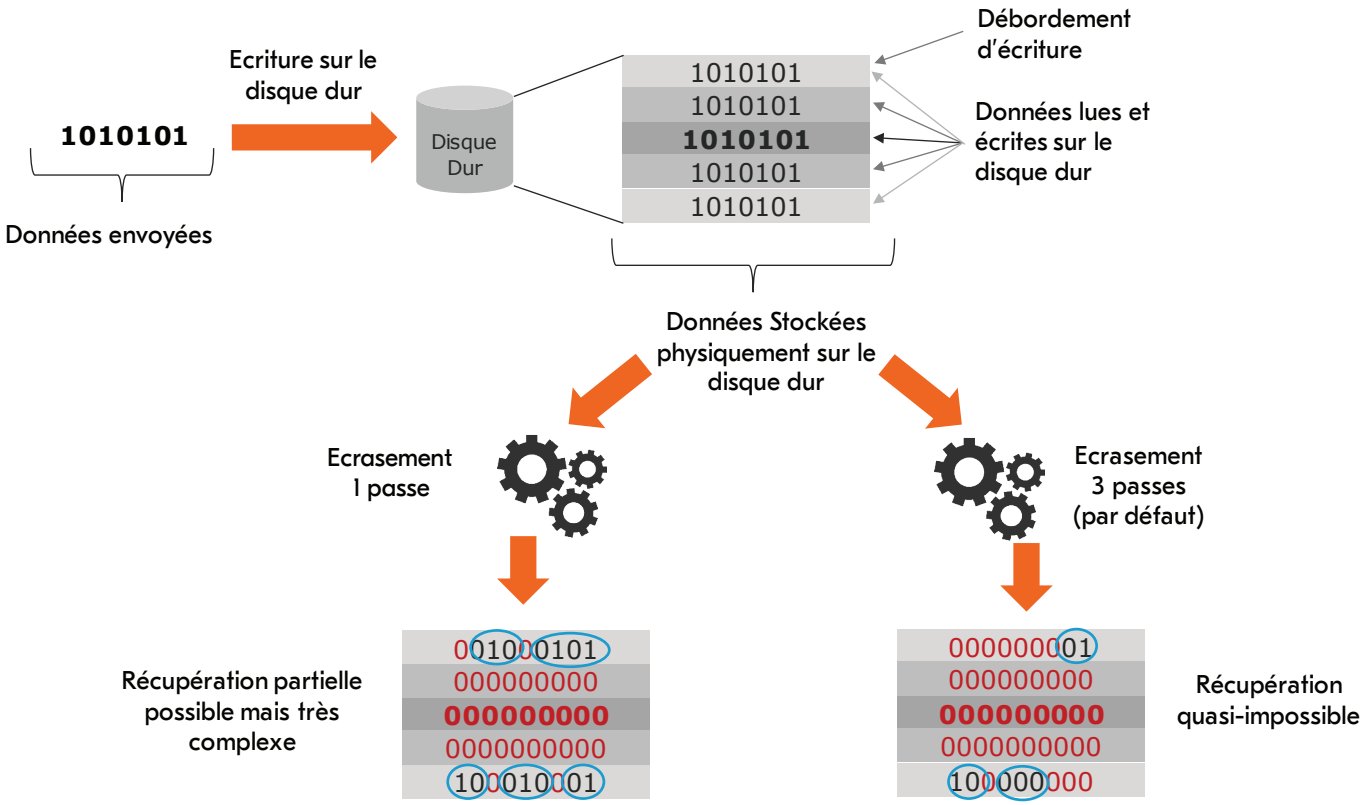
Ce souci de sécurisation des données se manifeste par l'ajout d'une puce TPM.
Le module TPM détient la clé de chiffrement racine qui est utilisée pour créer la clé de chiffrement du disque dur et des certificats. Cette clé de chiffrement racine et la clé de chiffrement du disque dur sont rigoureusement protégées dans le TPM afin qu'elles ne puissent pas être divulguée sen dehors de la puce de sécurité. Par ailleurs, la clé de chiffrement du disque dur et la clé de chiffrement racine sont enregistrées séparément. Même si le disque dur est retiré du MFP, les données stockées sur le disque dur ne peuvent pas être divulguées et sont protégées en toute sécurité.

4.1.3 Écrasement - effacement de disque dur (en standard ou en option selon les modèles)

La fonction Écrasement / effacement du disque dur empêche toute personne de lire des données stockées sur un disque dur, même après leur suppression.
Les données numérisées par un périphérique sont temporairement stockées sur le disque dur avant d'être transmises. Après leur transmission ou suppression
par l'utilisateur, les données sont encore présentes sur
le disque dur jusqu'à ce qu'elles soient écrasées par d'autres données. Comme il est possible de restaurer ces données restantes avec des outils spéciaux, elles présentent des risques de fuites de données. La fonction Écrasement - effacement du disque dur permet de remplacer les données restantes (après leur transmission ou suppression) par des données sans signification pour rendre très difficile ou impossible leur restauration selon la méthode appliquée.
L'exécution de cette fonction est automatique. Elle n'exige aucune opération manuelle. Les données restantes sont écrasées après chaque annulation de tâche ou à la fin de chaque travail d'impression complet ou de numérisation. Trois méthodes d'écrasement - effacement sont disponibles selon les modèles de périphériques Kyocera.

- **Méthode une passe**
  Des données nulles remplacent les données inutiles dans la zone des données temporaires, rendant très difficile leur restauration.

- **Méthode Trois passes**
  Des données aléatoires sont enregistrées deux
  fois dans la zone des données inutiles, avant une troisième passe qui enregistre des données nulles. Ces trois passes successives détruisent totalement les données et rendent très aléatoire leur récupération, même avec les techniques les plus sophistiquées. La méthode d'écrasement - effacement à trois passes est évidemment plus rigoureuse que la méthode à une passe.
  Mais elle peut exiger des durées plus longues, en particulier si les volumes à écraser-effacer sont importants.



4.1.4 Sécurisation des données en fin de vie

Lorsque des périphériques arrivent en fin de vie ou de location, les données privées, confidentielles ou sensibles qu'ils peuvent encore contenir sont exposées à des risques de fuite et de divulgation à des tiers. Pour éliminer ce type de risque, la fonction « Sécurisation des données en fin de vie » permet d'éliminer totalement les données grâce à différentes méthodes.

- **Méthode 3 passes**
  Des données aléatoires sont enregistrées deux fois dans la zone des données inutiles, avant une troisième passe qui enregistre des données nulles. Ces trois passes successives détruisent totalement les données et rendent très aléatoire leur récupération, même avec les techniques les plus sophistiquées. La méthode d'écrasement - effacement à trois passes est évidemment plus rigoureuse que la méthode à une passe.
- **Méthode 7 passes**
  L'écrasement à 7 temps est conforme à la méthode VSITR définie par l'Office fédéral allemand de la sécurité des informations (BSI) et écrase toutes les zones de données du disque dur. Toutes les zones de données sont écrasées avec des zéros (0x00), puis avec la valeur fixe (0xff). Cette opération sera effectuée trois fois de manière répétée. Ensuite, les zones de données seront écrasées avec la valeur fixe (0xAA). Ainsi, même avec un processus de restauration sophistiqué, il serait extrêmement difficile de restaurer les données complètement effacées. Les données sont écrasées sept fois.

4.2 Restriction d'accès

Les utilisateurs peuvent créer dans leurs périphériques des "Boîtes perso", des "Boîtes de tâches" et des "Boîtes Fax" pour stocker des données. Les accès à ces boîtes peuvent être contrôlés de différentes manières décrites ci-dessous.

4.2.1 Boîte Personnalisée

Les utilisateurs peuvent créer une «Boîte Personnalisée» (ou Boite Utilisateur) pour stocker des données sur un ou plusieurs périphériques. Des restrictions d'utilisation, de conservation des données et des mots de passe peuvent être définis pour chaque boîte.

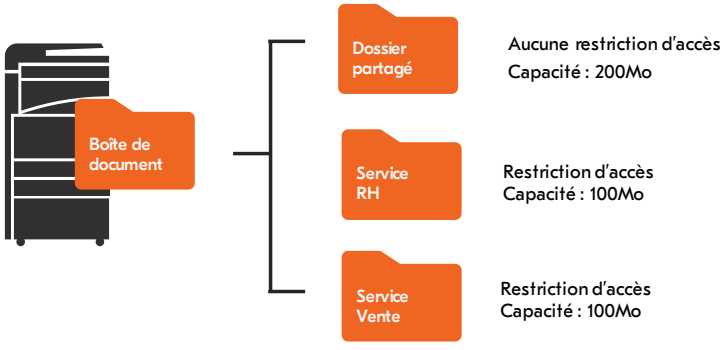
Mot de passe de la boîte
Les utilisateurs pouvant accéder à une boîte peuvent être contrôlés par un mot de passe. Ils doivent saisir un mot de passe correct pouvant contenir jusqu'à 16 caractères (incluant majuscules, minuscules, chiffres, signes spéciaux).

Restriction d'utilisation de la boîte
La capacité réservée à chaque boîte peut être définie pour faciliter la gestion de l'espace de stockage.

Paramètres du propriétaire
Une Boîte Personnalisée peut uniquement être accessible par un utilisateur préalablement inscrit comme propriétaire. Elle est donc inaccessible par un utilisateur non-autorisé.
Le système permet de programmer si une boîte est ou non partagée ("Boîte partagée"). Si une boîte est partagée, un utilisateur non-inscrit comme propriétaire peut y accéder. Grâce à la facilité d'utilisation de cette fonction, les boîtes peuvent être efficacement protégées contre les accès non-autorisés. Le système permet de maintenir une sécurité efficace.

Période de conservation des documents
Après une période prédéterminée, les données documentaires peuvent être automatiquement effacées si leur conservation n'est pas nécessaire à long terme. En outre, cette mesure réduit les risques de fuites ou d'exposition des données à des tiers.

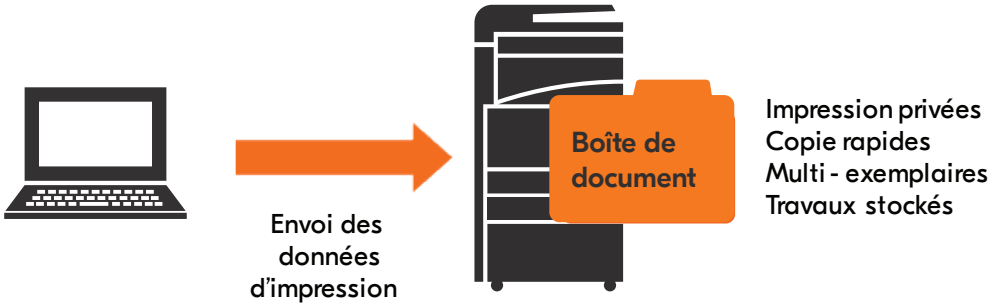
Délai de suppression des travaux stockés
Lorsqu'une tâche d'impression est terminée, les données des documents sont automatiquement supprimées dans la boîte concernée. La suppression des données ne peut donc pas être omise. Cette mesure évite les risques d'exposition des données à des tiers non-autorisés.



4.2.2 Boîte de travaux

Les données des «Impressions sécurisées», «Copies rapides», «Multi-exemplaires avec premier jeu d'essai» et «Travaux stockés» peuvent être stockées dans une Boîte de travaux, mais cette boîte ne peut pas être supprimée ou créée par un utilisateur. La boîte peut être protégée par un code PIN pour contrôler l'accès.

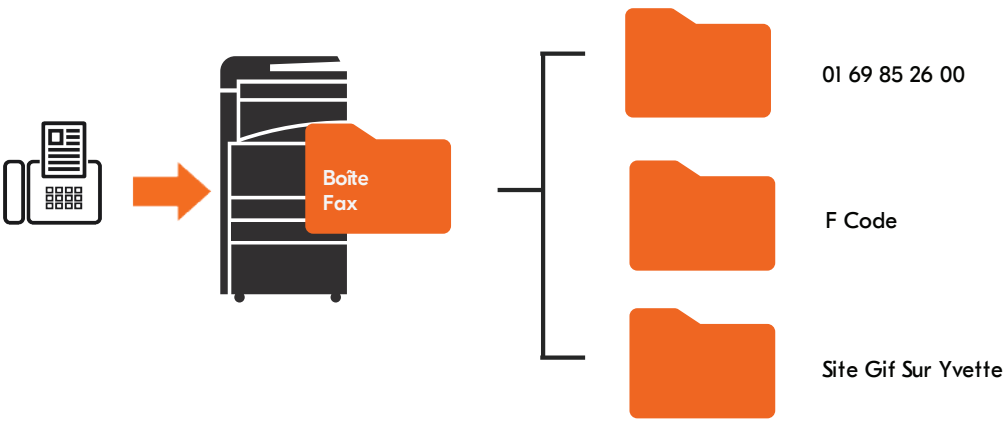
Suppression automatique des données temporaires
Les données temporairement enregistrées dans une boîte pour réaliser des «Impressions sécurisées», «Copies rapides», «Multi-exemplaires avec premier jeu d'essai» peuvent être automatiquement supprimées après un délai prédéterminé. Les données sont uniquement conservées pendant la période programmée. Les risques d'exposition des données à des tiers sont donc très largement réduits.



4.2.3 Boîte de Fax

Cette boîte permet de stocker des données reçues par télécopie sur un multifonction. Les télécopies reçues peuvent être conservées dans la boîte de Fax à l'aide de la fonction Transfert sur mémoire. Les télécopies reçues sont attribuées à leurs boîtes respectives en fonction des sous-adresses des expéditeurs ou numéros de fax, supportant une confirmation rapide des documents importants. Les télécopies reçues peuvent être confirmées sur le panneau de commande du multifonction. Les fax sélectionnés peuvent être imprimés immédiatement ou supprimés.

Mot de passe de la boîte
Un mot de passe peut être défini pour pouvoir accéder à une boîte. Les utilisateurs doivent saisir un mot de passe correct pouvant contenir jusqu'à 16 caractères (incluant majuscules, minuscules, chiffres, signes spéciaux).



Paramètres du propriétaire
Une boîte peut uniquement être accessible pour un utilisateur préalablement inscrit comme propriétaire. Elle est donc inaccessible par un utilisateur non-autorisé. Le système permet d'indiquer si une boîte est ou non partagée ("Boîte partagée"). Si une boîte est partagée, un utilisateur non-inscrit comme propriétaire peut y accéder. Les boîtes peuvent être efficacement protégées contre les accès non-autorisés. Le système permet donc de maintenir une sécurité efficace.

Suppression automatique des données
Lorsqu'une tâche est terminée, les données reçues et enregistrées dans une boîte peuvent être automatiquement supprimées. La conservation prolongée de données sans nécessité expose à des risques de fuite de données. La suppression rapide des données renforce la sécurité.

5 Sécurité des impressions

5.1 Sécurité des impressions

La fonction Sécurité des impressions fait partie des fonctions d'impression offertes par les périphériques Kyocera. Elle peut servir à imprimer des fichiers confidentiels ou des fichiers personnels en évitant de laisser des documents imprimés sans surveillance ou exposés à la vue de tous sur un dispositif.

5.1.1 Impression sécurisée

La fonction Impression sécurisée permet de conserver une tâche d'impression dans un périphérique jusqu'à ce qu'un utilisateur saisisse le mot de passe correct sur le panneau de commande du périphérique.
L'utilisateur doit définir un code d'accès dans le pilote de l'imprimante lorsqu'il envoie la tâche d'impression depuis un ordinateur. Il devra saisir ce même code sur le panneau de commandes du dispositif pour lancer l'impression.
Lorsque l'impression est terminée, les données sont automatiquement supprimées. Les données sont supprimées même si le dispositif est éteint avant l'impression. Cette fonction apporte un niveau de sécurité relativement élevé sur les dispositifs d'impression.

5.2 Prévention de copie non-autorisée

Pour réaliser des copies, les fonctions suivantes peuvent prévenir des copies non-autorisées grâce à des fonctions de sécurité documentaire avancées.

5.2.1 Filigrane (ou marquage)

La fonction Filigrane permet d'ajouter une marque sur le document imprimé qui signale au premier coup d'œil l'importance du document (ou son niveau de confidentialité). Les utilisateurs peuvent sélectionner diverses mentions imprimables en filigrane, telles que «Confidentiel», «Ne pas copier» «Personnel» ou autres selon les filigranes disponibles sur le modèle. En outre, ces filigranes peuvent être librement modifiés par les utilisateurs. Cette fonction permet aussi d'imprimer en filigrane un numéro de série ou des numéros de page.

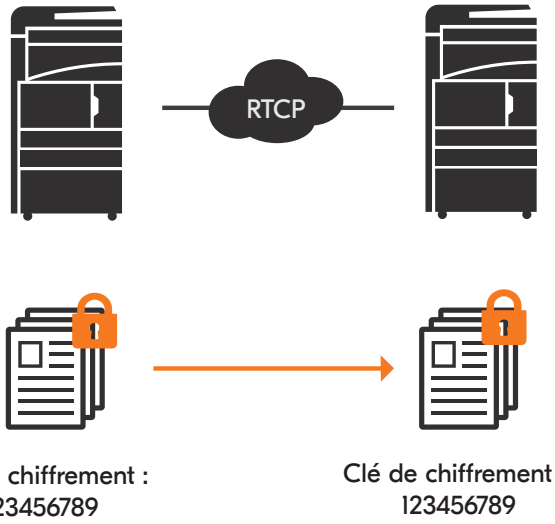
5.2.2 Filigrane de sécurité

Un filigrane de sécurité contenant un texte ou un graphisme peut être intégré dans un document. Le filigrane de sécurité intégré à un document est visible sur chaque copie. Il prouve que l'impression du document n'a pas été autorisée.
Sur le document imprimé original, un motif de fond sera imprimé et permet de masquer le filigrane de sécurité.
La copie de ce document mettra en évidence le filigrane de sécurité par contraste.

6 Sécurité des télécopies

6.1 Fax chiffré

Cette méthode de communication permet de chiffrer les données avant leur envoi. Par conséquent, les données restent inaccessibles à des tiers pendant leur transmission sur le réseau public. Aucun tiers ne peut lire et prendre connaissance de leur contenu. Les données reçues doivent être déchiffrées avant d'être imprimées par le destinataire. Cette méthode offre une sécurité efficace pour transmettre par fax des documents sensibles et confidentiels.
Elle est uniquement disponible entre deux périphériques Kyocera supportant la même fonction de Fax chiffré.
La même clé de chiffrement est utilisée pour chiffrer et déchiffrer les données sur les périphériques en émission et réception. Si les périphériques en émission et réception n'ont pas la même clé, la communication chiffrée ne peut avoir lieu. Les utilisateurs des périphériques doivent donc déterminer et enregistrer la même clé de chiffrement (chiffrement symétrique) avant d'utiliser cette fonction.



6.2 Restriction d'envoi / réception

Cette fonction autorise uniquement un périphérique à envoyer et/ou reTCPcevoir des télécopies si des conditions prédéterminées sont satisfaites, telles que numéro de fax autorisé et identifiant autorisé.
Elle permet donc de contrôler les destinataires des télécopies.
Lorsque la Restriction de réception est appliquée conjointement à une liste d'expéditeurs refusés, un fax envoyé par un expéditeur figurant sur cette liste ou qui n'a pas enregistré un numéro de fax, sera refusé.
Les fax peuvent uniquement être envoyés aux destinations enregistrées sur une liste de numéros et un carnet d'adresses.

6.3 Prévention de transmission non-autorisée

Pour éviter que des documents importants puissent être transmis à des destinations non-autorisées, les utilisateurs doivent saisir deux fois le numéro de fax du destinataire avant l'envoi.

La destination précédente n'est pas conservée, évitant donc la transmission d'un autre document à la dernière destination utilisée.

Cette fonction prévient efficacement les fuites d'informations parce que les destinations ne peuvent pas être lues par des tiers. Les informations concernant la destination d'envoi sont supprimées immédiatement après la déconnexion lorsque l'authentification d'utilisateur est activée.

6.3.1 Confirmation de saisie

Les utilisateurs doivent saisir deux fois le même numéro de fax sur les touches numériques pour le confirmer avant d'envoyer un fax.
Le numéro du destinataire est uniquement activé lorsque le numéro de fax est saisi deux fois sans erreur et donc confirmé.
Cette mesure élimine les risques de transmission erronée, causés par des erreurs de saisie.

6.3.2 Interdiction de saisie directe des numéros de fax sur les touches numériques

Contrôlée sur le panneau de commandes, cette fonction permet de restreindre la saisie directe sur les touches numériques. Elle permet aux utilisateurs d'envoyer uniquement des fax aux destinations enregistrées sur une liste préenregistrée.
Les utilisateurs **peuvent uniquement** envoyer des fax aux destinataires listés dans le carnet d'adresses ou enregistrés sur les touches de la numérotation rapide.
Cette fonction prévient donc les transmissions erronées causées par des numéros erronés ou des utilisations non-autorisées.

6.3.3 Confirmation avant envoi

Lorsque l'utilisateur appuie sur la touche [Départ], les destinations sont affichées sur l'écran, permettant de les vérifier avant l'envoi. La touche de confirmation est uniquement activée lorsque toutes les destinations ont été correctement affichées. Comme les utilisateurs peuvent confirmer les destinations avant d'envoyer des fax, la fonction sert aussi à prévenir les erreurs de saisie et donc les transmissions erronées.

6.4 Interdiction temporaire

Cette fonction de sécurité définit la durée pendant laquelle l'impression des fax reçus est désactivée. Lorsque l'interdiction temporaire est activée, toutes les opérations telles que l'impression, la copie, la réception de messages ou USB, la transmission, la télécopie et l'impression de télécopie, sont indisponibles pendant cette durée.
Cette fonction est protégée par un code PIN et peut être temporairement annulée. Elle prévient toute utilisation non-autorisée des périphériques, par exemple l'impression de données pendant la nuit lorsque le personnel est réduit ou absent.

6.5 Communication des sous-adresses

La fonction Communication des sous-adresses permet d'envoyer et de recevoir des données avec une sous-adresse et un mot de passe, conformément à la recommandation de l'ITU-T (International Telecommunication Union Telecommunication Standardization Sector).
Cette fonction supporte des communications avec d'autres équipements compatibles ITU-T, incluant les communications confidentielles (ex. communication destinée à une boîte spécifique du périphérique destinataire) ou les communications par cycle d'appel (pour recevoir le document original sur le périphérique expéditeur grâce à une commande exécutée sur celui du destinataire) et qui ont été longtemps uniquement disponibles sur des périphériques Kyocera.
Lorsque la fonction Communication des sous-adresses est activée, les données reçues sont enregistrées dans la boîte des sous-adresses.
Cette fonction contribue à améliorer la sécurité des communications.

6.5.1 Transmission confidentielle des sous-adresses

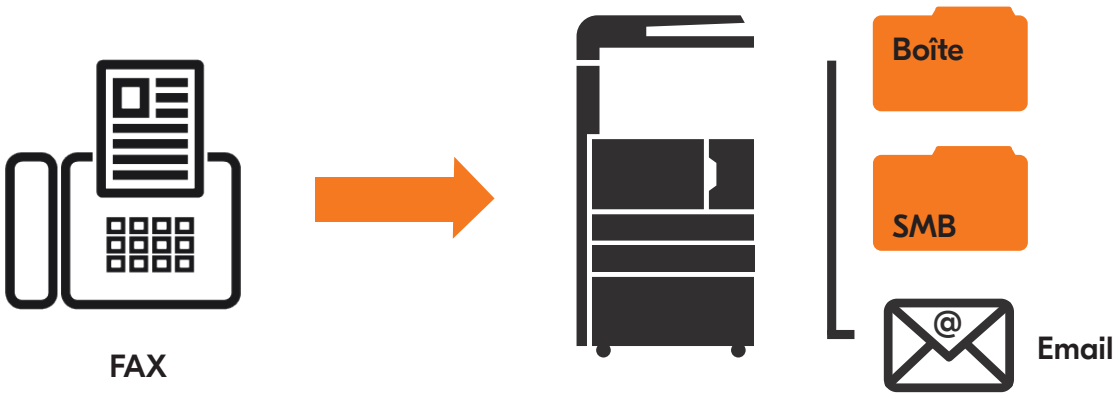
Lorsqu'une boîte confidentielle de sous-adresses est créée sur le périphérique destinataire, il est possible d'envoyer dans cette boîte un document important protégé par une sous-adresse et un mot de passe. Le document reçu est enregistré dans la boîte sans avoir à l'imprimer immédiatement après sa réception. Le document reçu peut ainsi être imprimé sans qu'aucun tiers ne puisse le voir.

6.5.2 Transmission différée des sous-adresses

Lorsque les périphériques destinataires supportent la fonction Transmission différée des sous-adresses, la transmission du document est protégée sans risque de divulgation.

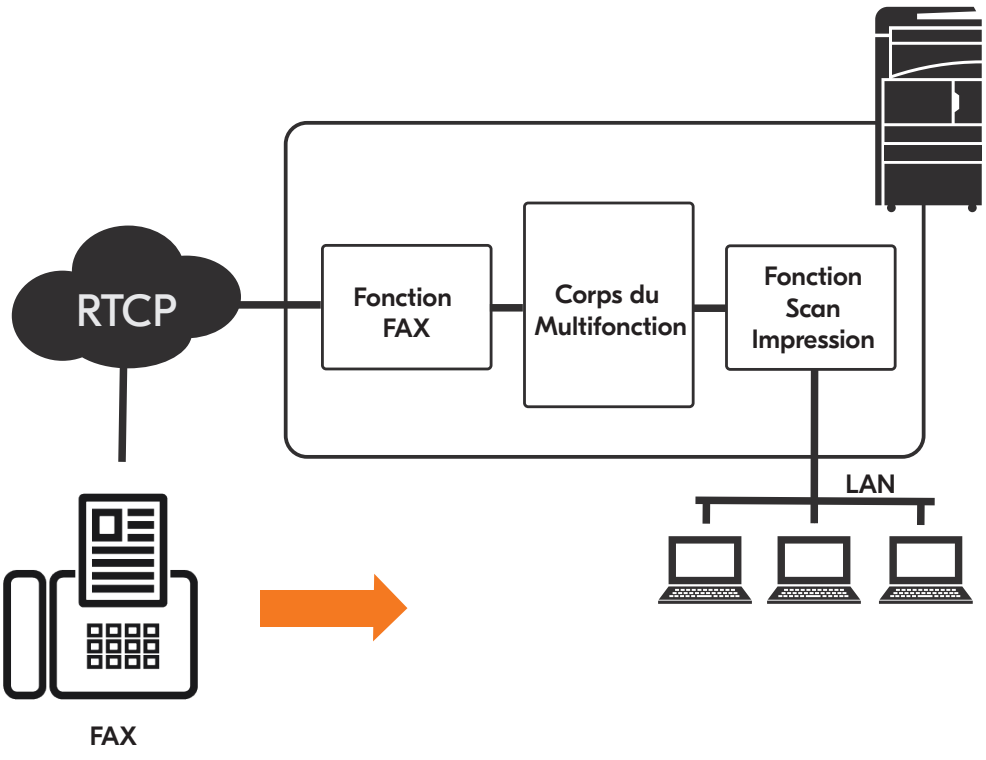
6.6 Transfert sur mémoire

Grâce à cette fonction, les images des documents reçus sont transférées aux autres télécopieurs ou ordinateurs, ou imprimés, dès la réception des fax.
Lorsque cette fonction est activée, toutes les images des documents reçus peuvent être transférées vers les adresses prédéterminées (destinations). Ceci peut être appliqué à un autre fax, mail, SMB et envoi FTP.
Les images des documents reçus peuvent aussi être transmises dans la boîte configurée sur un multifonction puis enregistrées. Ceci évite de laisser des documents reçus sans surveillance dans le bac du dispositif.



6.7 Mesure de sécurité contre les accès non-autorisé

La fonction Fax et la fonction Réseau sont structurellement séparées. Les données reçues sur une ligne téléphonique sont traitées par la fonction Fax. Cette structure interdit les accès non-autorisés au réseau depuis la ligne téléphonique connectée à la fonction Fax d'un multifonction.



7 Sécurité des envois

7.1 Confirmation de destination avant envoi

Les utilisateurs peuvent confirmer la destination (ex. numéros) et l'objet sur l'écran avant l'envoi. Elle contribue donc à prévenir les envois vers des adresses erronées. Ces informations peuvent être affichées sur le panneau de commandes avant l'envoi.

7.2 Saisies des nouvelles destinations

La saisie directe sur le panneau de commandes est limitée aux seules destinations préalablement enregistrées dans une liste, telle qu'un carnet d'adresses ou les touches de numérotation rapide. Cette fonction prévient efficacement les utilisations non-autorisées, erronées ou causées par des erreurs de saisie.

7.3 PDF Chiffré

La fonction PDF Chiffré permet aux utilisateurs de choisir le format de fichier PDF ou PDF compressé, de chiffrer les données numérisées et de sélectionner un mot de passe. Cette protection peut être appliquée à l'ouverture, l'impression ou la modification du fichier PDF reçu en saisissant le mot de passe correct.

7.4 Envoi de PDF Chiffré

La fonction Envoi de PDF Chiffré utilise TLS pour chiffrer le canal de communication. Les données transmises sont protégées. Cette fonction réduit considérablement les risques d'accès ou de modifications illicites des données en transit.

7.5 Signature numérique du fichier

Cette fonction permet aux utilisateurs de renforcer la sécurité en ajoutant une signature numérique aux fichiers. Un certificat de périphérique et une paire de clés privées/publiques sont enregistrés à l'avance dans le MFP Kyocera. Après la numérisation, le certificat du périphérique et la paire de clés sont utilisés pour générer une signature numérique, puis un fichier avec la signature numérique est généré par le MFP. Ce processus permet au destinataire de vérifier quel MFP a généré le fichier avec la signature numérique, et si le fichier a été modifié après avoir été généré avec cette signature numérique.

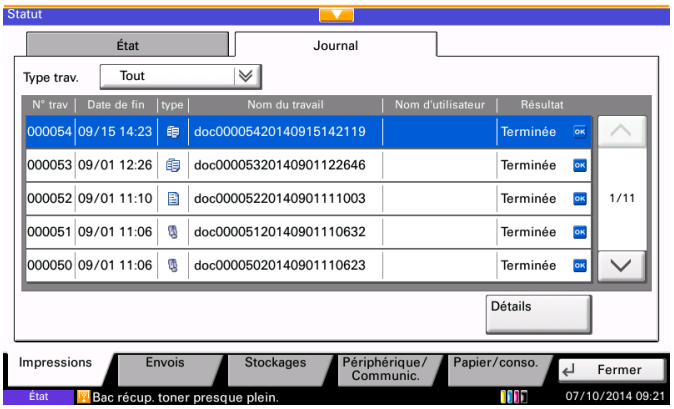
7.6 Envoi chiffré par FTP

L'envoi chiffré par FTP est effectué en utilisant TLS chiffrer le canal de communication. Ainsi, les données en transit restent sécurisées. Cela permet de minimiser fortement les risques de modification des données en transit ou d'écoute électronique.

8 Administration de dispositifs

8.1 Gestion des travaux

Les données concernant les travaux en attente ou dans les journaux peuvent être vérifiées directement sur le périphérique.
4 statuts sont disponibles :
“Travaux imprimés”, “ Travaux envoyés”, “ Travaux stockés”, “ Travaux réservés” ;
Des informations détaillées sur les travaux spécifiques, incluant nom d’utilisateur, heure, destination, peuvent être consultées et exploitées à des fins d’audit.
Avec l’utilisation du pilote d’impression KX, l’utilisateur peut choisir d’associer ou non, le fichier avec le nom du travail d’impression (afin de garantir la confidentialité dans les journaux par exemple)



8.1.1 Autorisation d’accès aux historiques depuis le panneau de commandes

Le journal des travaux peut être accessible en fonction des droits de l’utilisateur.
Les droits de consultation des journaux des travaux et des fax sont définis pour les états des tâches et le journal des tâches, respectivement.
Lorsque l’authentification des utilisateurs est activée, seul l’utilisateur autorisé peut afficher et vérifier les journaux avec ses propres travaux uniquement.
Toutes les informations concernant le journal des travaux sont affichées si l’utilisateur est connecté comme administrateur.

8.2 Rapport d’audit

Le système permet de générer un rapport d’audit des périphériques. Le journal d’utilisation du dispositif contient le nom d’utilisateur, les dates et heures et les statuts.
Le rapport d’audit couvre le journal des connexions, le journal du périphérique et le journal des erreurs de communication.
Grâce à ces rapports, l’administrateur des périphériques peut vérifier si chaque périphérique est utilisé de manière sécurisée ou est exposé à des risques.

8.2.1 Journal des accès (historique des connexions)

Le journal des accès (ou historique des connexions) avec les informations liées à l’authentification des utilisateurs peut être enregistré. En cas d’activité non-autorisée, de modification, de fuite de document sur un périphérique, ce journal permet d’enquêter et de tracer les accès non-autorisés à des fins d’audit.

8.2.2 Journal du périphérique (journal machine)

Les modifications des paramètres du périphérique et les mises à jour du firmware sur les périphériques peuvent être enregistrées.
Les modifications effectuées à partir du menu du système par l’administrateur sont également enregistrées.
Ce journal permet également de retracer toutes les modifications pour des analyses en cas de dysfonctionnement dû à un changement d’un technicien/utilisateur ou administrateur.

8.2.3 Journal des erreurs de communication sécurisée

L'administrateur peut confirmer si la communication de réseau est correctement exécutée en consultant le journal des erreurs de communication et de la sécurité du réseau. Si des erreurs de communication fréquentes sont constatées, les accès non-autorisés potentiels peuvent être examinés en détail.

8.3 Gestion des journaux

La gestion des journaux permet de gérer le rapport d'audit et les journaux des travaux. Elle sert à identifier les sources potentielles des incidents de sécurité.

8.3.1 Envoi des journaux par courriel

Les différents journaux peuvent être envoyés par courriel à l'adresse électronique spécifiée par l'administrateur lorsque le nombre d'entrée dans les journaux atteint un nombre prédéterminé. Le format des fichiers transmis est XML.

8.3.2 Syslog (selon les modèles)

Grâce au protocole Syslog, lequel est implémenté dans les périphériques Kyocera, un journal d'audit pour les MFP/imprimantes peut être envoyé à un serveur SIEM (Security Information and Event Management)* en temps réel. Le journal d'audit peut être collecté et géré de manière centralisée. En outre, les menaces potentielles pour la sécurité peuvent être immédiatement détectées et analysées. Lorsque des tentatives d'accès non autorisées proviennent de tiers, que des modifications non autorisées sont apportées aux paramètres des appareils ou que des anomalies telles que des fuites de données sont détectées, une notification est envoyée à un administrateur. Cela atténue les risques de sécurité et réduit la charge de travail de l'administrateur, améliorant ainsi la fiabilité de la sécurité et l'efficacité opérationnelle de l'administrateur.

* : Le serveur SIEM doit être configuré dans l'environnement de l'utilisateur.

8.4 Vérification de l'intégrité des fonctions de sécurité

Les fonctions suivantes sont utilisées pour vérifier l'intégrité des fonctions de sécurité des périphériques Kyocera. Elles permettent de vérifier que les modules d'exécution des fonctions de sécurité n'ont pas été modifiés et qu'ils fonctionnent correctement. De même, l'intégrité des données que les fonctions de sécurité utilisent peut être vérifiée.

8.4.1 Vérification du logiciel

Cette fonction sert à vérifier si les modules d'exécution des fonctions de sécurité ont été modifiés et fonctionnent correctement.
En outre, l'intégrité des données utilisées par les fonctions de sécurité peut être vérifiée.

8.4.2 Micrologiciel signé numériquement

Une signature numérique est attachée au micrologiciel (firmware) pour assurer sa validité.
Le micrologiciel contrôle le fonctionnement des périphériques. Le micrologiciel signé numériquement empêche la modification par des personnes malveillantes. Les périphériques peuvent être protégés contre les dommages et l'utilisation non autorisée en vue de s'introduire dans les réseaux par rebond.

8.4.3 Démarrage sécurisé (Secure Boot)

Secure Boot est une fonction qui permet de s'assurer qu'un matériel démarre en utilisant le micrologiciel autorisé avant son exécution. La validité du micrologiciel peut être vérifiée en appliquant une signature numérique au micrologiciel. Lorsque le périphérique démarre, le micrologiciel est chargé dans la RAM. À ce moment-là, il est confirmé que la valeur de hachage du microprogramme téléchargé sur le matériel et la valeur de hachage créée à partir de la signature sont identiques. Même si une personne malveillante crée un micrologiciel non autorisé, celui-ci ne peut pas passer la vérification de validité à l'aide de la signature numérique. Par conséquent, même si un micrologiciel est modifié par une personne malveillante, il ne peut jamais être exécuté.

8.4.4 Contrôle d'intégrité en cours de fonctionnement (RTIC)

La fonction Run Time Integrity Check est une fonction qui vérifie régulièrement la validité du micrologiciel pendant le fonctionnement du MFP sans altérer le micrologiciel chargé dans la RAM. Même si le micrologiciel est malicieusement réécrit, il peut être détecté et un avertissement est émis sous la forme d'une erreur système. Combinée à la fonction Secure Boot, la fonctionnalité de contrôle d'intégrité en cours de fonctionnement renforce la protection des périphériques contre les tentatives de piratage par modification de micrologiciel.

8.4.5 Vérification des micrologiciels à la demande

Enfin, l'intégrité du micrologiciel peut être vérifiée à la demande. Si un attaquant tente de charger un micrologiciel corrompu, un avertissement sera émis. En cumulant vérification du micrologiciel à la demande, au démarrage et en cours d'exécution, vous assureŴ vos utilisateurs de disposer de périphériques très sécurisés.

8.4.6 Vérification des logiciels autorisés par liste blanche (selon les modèles)

Ìnfin, l'intégrité du micrologiciel peut être vérifiée à la demande. Si un attaquant tente de charger un micrologiciel corrompu, un avertissement sera émis. Ìn cumulant vérification du micrologiciel à la demande, au démarrage et en cours d'exécution, vous assureŴ vos utilisateurs de disposer de périphériques très sécurisés.

8.*5* Restriction d'utilisation

8.5.1 Blocage d'interface

L'accès à l'interface du périphérique peut être bloqué. Ce blocage peut être appliqué à un dispositif USB, un hôte USB, une interface optionnelle (port 1) une deuxième interface optionnelle (port 2). L'interface du réseau peut être restreinte par le paramétrage des protocoles réseau.

8.5.2 Blocage logique des ports USB

La connexion d'un support de stockage USB à un port USB sur un périphérique crée des risques de fuites de données ou d'accès non-autorisés aux informations.
L'administrateur peut désactiver les ports USB, tout en autorisant la connexion d'un lecteur de badges USB sur l'interface hôte USB des périphériques.
Les périphériques Kyocera sont dotés d'une fonction qui permet de restreindre l'utilisation des stockages USB, même si une clé USB est insérée dans l'interface hôte USB des périphériques. Cette fonction prévient les fuites de données et la propagation de menaces potentielles par l'interface USB.

8.5.3 Verrouillage du panneau de commandes

Les opérations réalisées à partir du panneau de commandes des périphériques peuvent être restreintes.
Le verrouillage du panneau de commandes permet de bloquer l'utilisation du menu système et d'annuler des travaux par exemple. Ce verrouillage interdit les opérations non-autorisées sur les périphériques.

Item	Verrouillage partiel	Verrouiller
Accès au mode maintenance	Interdit	Interdit
Accès au menu système	Interdit	Interdit
Transmission depuis les boîtes de document	Interdit	Interdit
Ajouter/Editer dans le carnet d'adresses	Interdit	Interdit
Ajouter/Editer une boîte de document	Interdit	Interdit
Appuyer sur le bouton Stop	Autorisé	Interdit
Accès au Statut/ annulation des travaux	Autorisé	Interdit
Déconnecter les lignes Fax	Autorisé	Interdit

Il existe sur certains modèles plusieurs modes de verrouillage partiel.

Kyocera Document Solutions est pionnier des technologies innovantes depuis 1934. Nous permettons à nos clients de transformer les informations en connaissances, d'exceller dans l'apprentissage et de surpasser les autres. Avec une expertise professionnelle et une culture de partenariat empathique, nous aidons les organisations à mettre leurs connaissances au service du changement.

KYOCERA Document Solutions France S.A.S.

Espace Technologique de Saint-Aubin, Route de l'Orme,
91195 Gif-sur-Yvette cedex, France
Tél. : +33 (0) 1 69 85 26 00

KYOCERA

kyoceradocumentsolutions.fr