Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234234

3 juillet 2022

Sommaire

Vue d'ensemble du document

Ce document fournit des informations sur la manière dont les technologies et les fonctions de sécurité sont implémentées dans Fiery FS500 Pro/FS500 servers et couvre la sécurité matérielle, la sécurité du réseau, le contrôle d'accès, les systèmes d'exploitation et la sécurité des données. L'objectif du document est d'aider nos clients à combiner les technologies de sécurité de la plate-forme Fiery avec leurs propres stratégies pour répondre à leurs exigences de sécurité spécifiques.

Conventions terminologiques

Ce document utilise la terminologie suivante pour désigner le Fiery FS500 Pro/FS500 servers, les imprimantes et les applications Fiery.

Terme ou convention	Signification
Fiery server	Fiery FS500 Pro/FS500 servers
Imprimante	Imprimante, copieur, presse numérique, presse ou dispositif de sortie
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	Logiciel Fiery QuickTouch s'exécutant sur le panneau LCD du serveur Fiery

Philosophie de sécurité d'EFI

EFI a conscience que la sécurité est l'une des principales préoccupations des organisations et entreprises du monde entier. Nos produits sont régulièrement améliorés grâce à des fonctions de sécurité renforcées destinées à protéger les biens de votre entreprise. Les Fiery servers d'EFI sont conçus en intégrant la sécurité en tant que composant principal pour protéger les données système lors de leur repos, en transit et pendant leur traitement.

En travaillant en étroite collaboration avec nos partenaires et fournisseurs EFI mondiaux, nous nous engageons à soutenir continuellement nos clients en leur apportant des solutions, à mesure que les menaces évoluent. Afin de garantir la sécurité globale du système, nous recommandons aux utilisateurs finaux d'allier les fonctions de sécurité Fiery avec les stratégies de sécurité de leur propre entreprise et les meilleures pratiques spécifiques au secteur, comme les mots de passe sécurisés et les procédures de sécurité physique fortes.

Objectifs de sécurité EFI

EFI s'est fixé les objectifs suivants concernant la mise en œuvre des mesures de sécurité pour le Fiery server :

- **Sécurité des données** : pas de divulgation non autorisée de données pendant le traitement, la transmission (en transit) ou la conservation (au repos).
- **Disponibilité** : performance telle que prévue, sans manipulation non autorisée.
- **Contrôle d'accès** : pas de déni de service aux utilisateurs autorisés.
- **Maintenance conviviale** : notifications automatiques et téléchargements lorsque des mises à jour de sécurité sont disponibles.
- **Conformité** : prise en charge des réglementations industrielles et infrastructures de sécurité.

Mises à jour de sécurité du logiciel Fiery

Cette section offre un aperçu général du processus de mise à jour de la sécurité logicielle de Fiery server. Les vulnérabilités de sécurité du système d'exploitation Microsoft® Windows™ ne sont pas décrites car elles sont gérées directement par Microsoft et livrées en tant que mises à jour Windows dès qu'elles sont disponibles. Pour des problèmes de sécurité ou des vulnérabilités susceptibles d'avoir une incidence sur les composants matériels principaux de Fiery, tels que la carte mère, le processeur, le BIOS, etc., EFI collabore étroitement avec les fabricants pour obtenir les mises à jour de sécurité requises.

- EFI consulte le bulletin hebdomadaire de cybersécurité US-CERT de l'agence sur la cybersécurité et la sécurité des infrastructures (CISA). Ce bulletin résume les nouvelles vulnérabilités qui ont été enregistrées par la base de données de la vulnérabilité nationale (NVD) de l'Institut national des normes et de la technologie (NIST) au cours de la semaine qui précède. Les vulnérabilités sont fondées sur la norme de dénomination des vulnérabilités et expositions communes (CVE) et sont organisées en fonction de la sévérité (élevée, moyenne et faible) déterminée par le système de notation de vulnérabilité commun (CVSS).
- EFI fournit des correctifs de sécurité pour chaque plate-forme du Fiery server dès que possible.
- Les mises à jour de sécurité du logiciel Fiery sont envoyées aux partenaires EFI spécifiques pour approbation.
- Lorsqu'elles sont approuvées par les partenaires, les mises à jour de sécurité du logiciel Fiery sont disponibles au téléchargement.
- La mise à jour du système Fiery télécharge et installe les mises à jour de sécurité si l'option est activée sur le Fiery server. Cette option est activée par défaut et nous recommandons à nos clients de la laisser activée.

La mise à jour en temps voulu des logiciels est essentielle au fonctionnement optimal des Fiery servers. L'installation des mises à jour de sécurité logicielles pour Fiery et le système d'exploitation Windows est importante pour sécuriser les Fiery servers dans n'importe quel environnement d'impression donné.

Remarque : Toutes les mises à jour ou correctifs Fiery sont signés numériquement avec SHA-2.

Configuration des fonctions de sécurité du Fiery server

Configure est l'outil principal utilisé pour configurer les fonctions de sécurité des Fiery servers. Les administrateurs Fiery peuvent accéder à Configure à partir de la Command WorkStation ou des WebTools.

Remarque : Les utilisateurs doivent disposer des droits d'accès administrateur pour accéder à Configure.

Pour plus d'informations sur la configuration du Fiery server, voir Directives pour une configuration du serveur Fiery sécurisée à la page 32.

Sécurité matérielle

La sécurité matérielle du Fiery server consiste à éviter la perte de données en cas de panne de courant et l'accès non autorisé aux données situées sur un périphérique de stockage.

Mémoire volatile

Les données inscrites dans la mémoire vive volatile sont disponibles uniquement lorsque l'appareil est sous tension. Lorsqu'il est mis hors tension, toutes les données sont supprimées.

Pour plus d'informations, voir la Section mémoire volatile du tableau à la page 25.

Mémoire non volatile et stockage des données

Le Fiery server intègre plusieurs types de technologies de stockage de données non volatiles pour conserver les données lorsque le Fiery server est mis hors tension. Ces données se composent d'informations de programmation du système et de données d'utilisateur.

Pour plus d'informations, voir la Section mémoire non volatile du tableau à la page 25.

Mémoire flash

La mémoire flash stocke le programme d'autodiagnostic et d'amorçage (BIOS), ainsi que certaines données de configuration du système. La mémoire flash est programmée en usine et peut être reprogrammée uniquement en installant des correctifs spéciaux créés par EFI. Si les données sont corrompues ou supprimées, le Fiery server ne démarre pas.

CMOS

Disposant d'une batterie de sauvegarde, la mémoire CMOS permet de stocker les paramètres système du Fiery server. Ces informations ne sont pas considérées comme étant confidentielles ou privées. Lorsque la mémoire CMOS est installée, les utilisateurs peuvent accéder à ces paramètres sur un serveur sous Windows 10 IoT Enterprise 2016 ou 2019 à l'aide de l'écran, du clavier et de la souris.

NVRAM

Le Fiery server comporte plusieurs petits dispositifs NVRAM sur lesquels des microprogrammes opérationnels sont installés. Ces dispositifs contiennent des informations opérationnelles non spécifiques au client. L'utilisateur n'a pas accès à ces données.

Disque dur et lecteur à circuits intégrés (SSD)

Lors d'opérations normales d'impression et de numérisation, ou de la création des informations de gestion des tâches, les données d'image sont écrites dans une zone aléatoire du disque dur et du lecteur à circuits intégrés

Les données d'image et les tâches en file d'attente peuvent être supprimées manuellement par les utilisateurs à partir de la Command WorkStation, tout comme toute autre opération en file d'attente (comme les opérations affichées sur l'écran LCD de l'imprimante). Les données d'image et les objets peuvent également être supprimés automatiquement à l'aide de la commande **Effacer serveur**, ou lorsque le nombre de tâches imprimées dépasse les paramètres autorisés. La désactivation de la file d'attente d'impression supprimera également les tâches d'impression.

Pour protéger les données d'image contre tout accès non autorisé, EFI propose une fonctionnalité d'effacement sécurisé. Une fois cette fonctionnalité activée par l'administrateur Fiery, le mode opérationnel sélectionné est exécuté au moment approprié afin d'effacer de façon sécurisée les données supprimées du disque dur. L'effacement sécurisé de Fiery prend actuellement en charge uniquement les disques durs. Pour les lecteurs SSD, vérifiez les options d'assainissement du disque auprès du fabricant avant de procéder à leur effacement.

Remarque : Pour plus d'informations sur l'effacement sécurisé, voir Effacement sécurisé à la page 23.

Ports physiques

Le Fiery server peut être connecté via des ports externes illustrés dans les tableaux suivants :

Ports Fiery	Fonction	Accès	Contrôle de l'accès
Connecteur Ethernet RJ-45	Connectivité Ethernet	Connexions réseau	Utilisation du filtrage IP Fiery pour contrôler l'accès
Connecteur d'interface d'imprimante	Impression et numérisation	Dédié à l'envoi/la réception de données vers/depuis l'imprimante	Non applicable
Port USB	Connexion de périphériques USB Installation du logiciel système	Connecteur « plug-and-play » conçu pour une utilisation avec des périphériques de stockage amovibles en option	L'impression USB peut être désactivée. L'accès aux périphériques de stockage USB peut être désactivé via les stratégies de groupe de Windows. La fonction de stockage USB peut également être désactivée à partir de Configure.
Connecteur de fibre optique	Connectivité Ethernet 10 Go	Connexions réseau	Non applicable

Interface locale

Sur certains Fiery servers, l'utilisateur peut accéder aux fonctions Fiery via l'écran de la Fiery NX Station, ou via le logiciel Fiery QuickTouch sur l'écran tactile, ou encore via tout moniteur connecté au Fiery server. L'accès à la sécurité avec la Fiery NX Station sur le Fiery server est contrôlé par un mot de passe administrateur Windows. L'écran tactile permet d'accéder à des fonctions très limitées qui ne génèrent aucun risque de sécurité.

Kit de disque dur amovible en option

Certains Fiery servers prennent en charge, en option, un kit de disque dur amovible afin d'offrir un niveau de sécurité accru. Ce kit offre la possibilité de verrouiller le ou les disques du serveur dans le système en fonctionnement normal et de les extraire pour les mettre en lieu sûr une fois le Fiery server mis hors tension.

Pour les serveurs Windows autonomes

Les Fiery servers autonomes sous Windows prennent en charge un kit d'option pour disque dur amovible. La disponibilité de ce kit pour un produit Fiery spécifique dépend des termes des accords conclus par EFI avec chacun de ses partenaires Fiery.

Pour les serveurs Fiery XB

Les disques durs et les lecteurs à circuits intégrés sont amovibles sur les serveurs Fiery XB. La plupart des disques durs et des lecteurs à circuits intégrés sont couplés ensemble en configuration RAID. Il est important de replacer les disques dans leur emplacement d'origine afin d'éviter la perte de données et une nouvelle installation du logiciel système.

Activer les ports USB pour une utilisation de stockage

Les ports USB des Fiery servers autorisent la souris, le clavier ou les connexions au spectrophotomètre, mais ils empêchent les connexions aux périphériques de stockage USB lorsque l'option Activer la fonction de stockage USB est désactivée dans Configure. Cette option est activée par défaut. Lorsqu'elle est désactivée, elle désactive également les fonctionnalités Fiery nécessitant des fonctions USB de stockage de masse, comme Sauvegarde et restauration.

Sécurité du réseau

Le Fiery server dispose de diverses fonctions de sécurité réseau conçues pour contrôler et gérer l'accès à l'imprimante. Seuls les utilisateurs et groupes autorisés peuvent accéder au Fiery server et soumettre des impressions à l'imprimante. Le Fiery server peut également être configuré pour limiter ou contrôler les communications externes en utilisant des adresses IP désignées et en désactivant les ports et protocoles réseau. Les Fiery servers doivent toujours être déployés dans un environnement réseau protégé. L'accessibilité doit être correctement configurée et gérée par un administrateur réseau qualifié et autorisé.

Ports réseau

Par défaut, tous les ports TCP/IP non utilisés par des services Fiery spécifiques sont désactivés. L'administrateur Fiery peut sélectionner les ports réseau à activer ou désactiver. La désactivation d'un port réseau bloque les connexions extérieures qui utilisent le port spécifié. Si un port spécifique est activé, les connexions extérieures sont autorisées par le biais de ce port.

TCP	UDP	Nom du port	Services associés
20-21		FTP	FTP
80		HTTP	WebTools, IPP
135		MS RPC	Service Microsoft® RPC (Windows 10 uniquement). Un port supplémentaire compris entre 49152 et 65536 sera ouvert pour le service Pointer-imprimer associé au protocole SMB.
137-139		NETBIOS	Impression Windows
	161, 162	SNMP	Fiery Central, certains utilitaires plus anciens, autres outils SNMP
	427	SLP	SLP
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB par TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impression LPR, certains utilitaires plus anciens (tels que les versions antérieures de la Command WorkStation)
631		IPP	IPP
3389		RDP	Bureau à distance (serveurs Fiery sous Windows uniquement)

TCP	UDP	Nom du port	Services associés
3702	3702	WS-Discovery	WSD
	4500	IPsec par NAT	IPsec
	5353	DNS multidiffusion	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	Ports EFI	Command WorkStation 5 et 6, Fiery Central, outils SDK d'EFI, fonctions bidirectionnelles du pilote d'imprimante Fiery, WebTools, impression mobile directe Fiery et conversion de documents natifs
9100-9103		Port d'impression	Port 9100

Remarque : Les ports 50006-50025 sont activés une fois la Command WorkStation version 6.2 ou ultérieure installée sur un Fiery server autonome.

Les autres ports TCP sont désactivés, à l'exception de ceux spécifiés par le partenaire Fiery. Il est impossible d'accéder à distance à un service associé à un port désactivé.

L'administrateur Fiery peut également activer et désactiver les différents services réseau fournis par le Fiery server.

Filtrage IP

Le filtrage IP autorise ou refuse les demandes de connexion au Fiery server à partir d'adresses IP définies. L'administrateur peut définir des stratégies par défaut pour autoriser ou refuser les paquets de données entrants, et peut également spécifier des filtres pour un maximum de 16 adresses ou plages d'adresses IP pour autoriser ou refuser les demandes de connexion.

Chaque paramètre de filtre IP spécifie une adresse IP ou une plage d'adresses IP ainsi que l'action correspondante. Si l'action est refusée, les paquets contenant une adresse source appartenant aux adresses spécifiées seront supprimés. Si l'action est acceptée, les paquets seront autorisés.

Authentification réseau

SNMP v3

Le Fiery server prend en charge la dernière norme SNMPv3. Les paquets de communication SNMPv3 peuvent être cryptés afin de veiller à leur confidentialité, à l'intégrité et à l'authentification des messages.

L'administrateur Fiery a la possibilité de sélectionner l'un des trois niveaux de sécurité disponibles pour le protocole SNMP : minimal, moyen ou maximal. L'administrateur Fiery peut également exiger une authentification avant d'autoriser les transactions SNMP et de crypter les noms d'utilisateur et les mots de passe SNMP. L'administrateur

local peut définir des noms de communautés SNMP disposant de droits de communauté en lecture et en écriture, ainsi que d'autres paramètres de sécurité.

Pour plus d'informations, voir Paramètres recommandés à la page 32.

IEEE 802.1x

La norme 802.1x est un protocole IEEE standard pour le contrôle d'accès réseau basé sur des ports. Ce protocole assure l'authentification des périphériques avant que le Fiery server accède au réseau local (LAN) et à ses ressources.

Lorsque le protocole 802.1x est activé, le Fiery server peut être configuré de manière à utiliser la méthode EAP MD5-Challenge, PEAP-MSCHAPv2 ou EAP-TLS pour s'authentifier sur un serveur d'authentification 802.1x.

Le Fiery server s'authentifie au démarrage ou lorsque le câble Ethernet est débranché puis rebranché.

Chiffrement réseau

Internet Protocol Security (IPsec)

IPsec assure la sécurité de toutes les applications sur les protocoles IP par le cryptage et l'authentification de chaque paquet.

Le Fiery server utilise des clés d'authentification prépartagées pour établir des connexions sécurisées avec d'autres systèmes sur IPsec.

Une fois qu'une communication sécurisée est établie sur IPsec entre un ordinateur client et un Fiery server, toutes les communications, y compris les tâches d'impression, sont transmises de façon sécurisée sur le réseau.

HTTPS

Le Fiery server nécessite une connexion sécurisée entre les clients et les différents composants du serveur. HTTPS est utilisé avec TLS afin de crypter les communications entre les deux points terminaux. HTTPS est nécessaire lors de la connexion au Fiery server à partir des WebTools et de Fiery API. Ces communications sont chiffrées à l'aide des protocoles TLS 1.3 et 1.2.

Gestion de certificats

Les Fiery servers possèdent une interface permettant de gérer les certificats utilisés durant les communications TLS. Les Fiery servers prennent en charge le format de certificat X.509.

Les Fiery servers prennent en charge les certificats RSA avec une longueur de clé de 4096, 3072 et 2048 bits.

L'interface de gestion des certificats permet à l'administrateur Fiery d'effectuer les opérations suivantes :

- Créer des certificats numériques autosignés.
- Ajouter un certificat et la clé privée associée pour le Fiery server.
- Ajouter, parcourir, afficher et supprimer des certificats d'une autorité de certification approuvée.

Remarque : Les certificats autosignés ne sont pas sécurisés. Nous recommandons vivement aux utilisateurs d'utiliser un certificat émis par une autorité de certification de confiance.

Une fois que vous aurez obtenu un certificat signé par une autorité de certification de confiance, vous pourrez télécharger le certificat vers le Fiery server dans la section Configure des WebTools.

Sécurité e-mail

Le Fiery server prend en charge les protocoles de communication de messagerie POP et SMTP, lorsque la messagerie électronique est activée. (Cette fonction est désactivée par défaut.) Pour protéger le service contre les risques d'attaque et d'utilisation inappropriée, l'administrateur Fiery peut activer des fonctionnalités de sécurité additionnelles.

POP avant SMTP

Certains serveurs de messagerie électronique prennent toujours en charge le protocole SMTP non sécurisé, qui permet à quiconque d'envoyer des e-mails sans authentification. Pour prévenir tout accès non autorisé, certains serveurs de messagerie électronique exigent des clients qu'ils s'authentifient via le protocole POP avant d'utiliser le protocole SMTP pour envoyer un e-mail. Pour de tels serveurs, l'administrateur Fiery doit activer l'authentification POP avant SMTP.

OP25B

Le blocage du port 25 en sortie (OP25B, Outbound Port 25 Blocking) est une mesure antispam mise en œuvre par les fournisseurs d'accès à Internet pour bloquer l'accès des paquets au port 25 via leurs routeurs. L'interface de configuration de messagerie électronique permet à l'administrateur Fiery de spécifier un autre port.

Pour plus d'informations sur le flux de production d'impression par e-mail du Fiery server, voir Impression par e-mail à la page 26.

Serveur de messages SMB (Server Message Block)

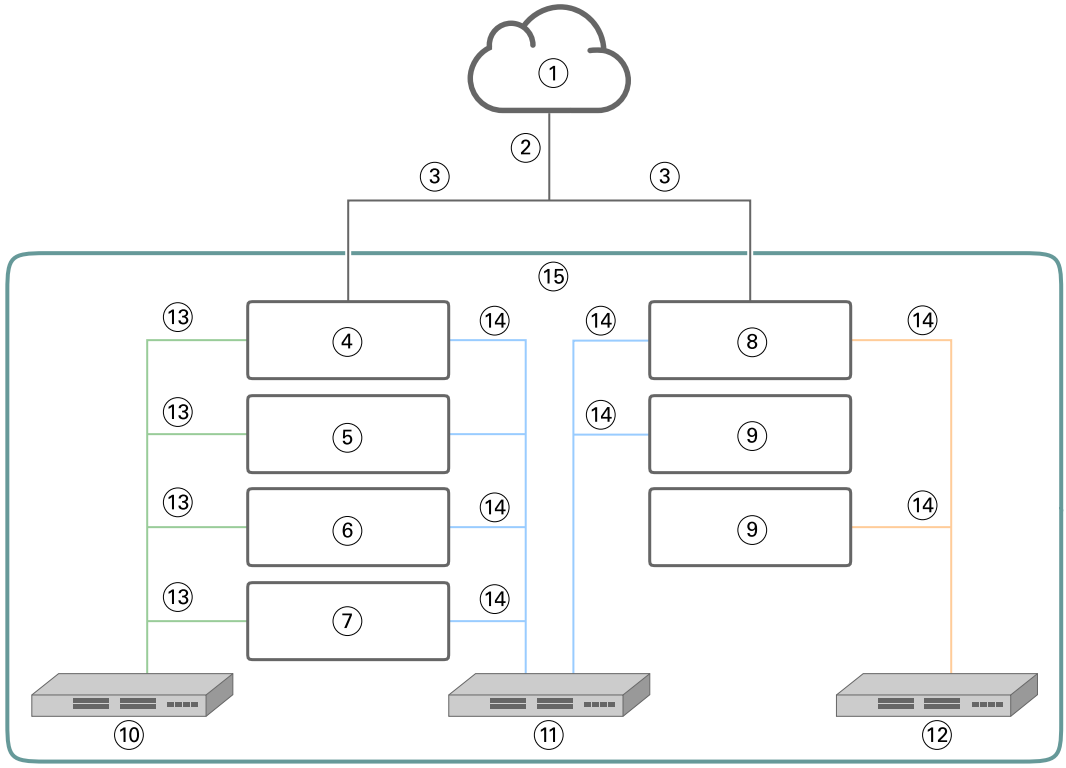
SMB est un protocole réseau qui permet de partager l'accès aux fichiers et aux imprimantes. SMB v1 est désactivé sur les Fiery servers car il ne répond pas aux normes de sécurité actuelles de l'industrie. SMB v2 et v3 sont toujours pris en charge.

La signature SMB est appliquée sur le Fiery server. La signature SMB nécessite des paquets signés numériquement pour permettre au destinataire de vérifier l'authenticité du paquet afin d'éviter les attaques de type « man-in-the-middle » (intermédiaire). Si l'authentification SMB est activée, l'utilisateur doit fournir le nom d'utilisateur et le mot de passe SMB pour accéder aux dossiers SMB et au contenu stocké dans les dossiers SMB.

Remarque : Il est possible de limiter l'impression ou le partage de fichiers via SMB en définissant un mot de passe dans Configure.

Diagramme de réseau Fiery XB

Le tableau suivant montre comment les serveurs Fiery XB et les imprimantes jet d'encre à grande vitesse se connectent au réseau.



1	LAN	9	Autres lames de presse (en option)
2	Trafic réseau de la gestion des tâches	10	Réseau privé 10 GbE
3	1 GbE DHCP ou statique	11	Réseau privé 1 GbE
4	Lame principale Fiery	12	Réseau privé CLP 1 GbE
5	Lame Fiery RIP (en option)	13	10 GbE
6	Lame Fiery n°1 (en option)	14	1 GbE
7	Lame Fiery n°2 (en option)	15	Environnement Fiery XB fermé
8	Lame de presse		

Contrôle de l'accès

Ce chapitre explique comment le Fiery server peut être configuré pour contrôler l'accès aux ressources pour différents groupes d'utilisateurs.

Authentification utilisateur

La fonctionnalité d'authentification d'utilisateur du Fiery server permet les opérations suivantes :

- Authentifier un utilisateur
- Autoriser l'utilisateur à réaliser des actions en fonction de ses privilèges

Le Fiery server peut authentifier les utilisateurs :

- reposant sur le domaine : utilisateurs définis sur un serveur d'entreprise et dont l'accès s'effectue via le protocole LDAP
- reposant sur le système Fiery : utilisateurs définis sur le Fiery server

Le Fiery server autorise certaines actions de la part des utilisateurs en fonction du groupe auquel ils appartiennent. Chaque groupe est associé à un ensemble de droits (par exemple, Imprimer en niveaux de gris, Imprimer en couleur ou en niveaux de gris) et les actions des membres du groupe sont limitées à ces droits. L'administrateur Fiery peut modifier les droits de tout groupe Fiery, à l'exception des comptes administrateurs et opérateurs.

Dans cette version de la fonctionnalité d'authentification d'utilisateur, les différents droits qui peuvent être sélectionnés pour un groupe sont les suivants :

- **Imprimer en niveaux de gris**: ce droit permet aux membres du groupe d'imprimer des tâches en niveaux de gris sur le Fiery server. Si l'utilisateur ne dispose pas de ce droit, le Fiery server n'imprimera pas la tâche. Si la tâche est en couleur, elle sera imprimée en niveaux de gris.
- **Imprimer en couleur et en niveaux de gris** : ce droit permet aux membres d'un groupe d'imprimer des tâches sur le Fiery server avec un accès total aux capacités d'impression couleur et niveaux de gris sur le Fiery server. Si l'utilisateur ne dispose pas de ce droit ou du droit Imprimer en niveaux de gris, l'impression de la tâche est impossible et l'utilisateur ne peut pas soumettre la tâche via FTP (périphériques couleur uniquement).
- **Boîte de messagerie Fiery**: ce droit permet aux membres d'un groupe de disposer de boîtes de messagerie individuelles. Le Fiery server crée une boîte de messagerie en fonction du nom d'utilisateur associé à ce droit. L'accès à cette messagerie s'effectue uniquement à l'aide du nom d'utilisateur et du mot de passe de la boîte.
- **Calibrage** : ce droit permet aux membres d'un groupe d'effectuer un calibrage couleur.
- **Créer des préréglages pour le serveur** : ce droit permet aux membres d'un groupe de créer des préréglages pour le serveur afin d'autoriser les autres utilisateurs du système Fiery à accéder aux préréglages couramment utilisés.

- **Gérer des flux de production** : ce droit permet aux membres d'un groupe de créer, publier ou modifier des imprimantes virtuelles.
- **Modifier les tâches** (serveurs Fiery XB uniquement) : ce droit permet aux membres du groupe de modifier une tâche dans la file d'attente.

Remarque : La fonctionnalité d'authentification utilisateur remplace les fonctionnalités d'impression réservée aux membres et d'impression groupée.

Authentification utilisateur du logiciel Fiery

Le Fiery server interagit avec différents types d'utilisateurs. Ces utilisateurs sont spécifiques au logiciel Fiery et ne sont pas liés aux utilisateurs ou aux rôles définis sous Windows. Il est recommandé aux administrateurs d'exiger des mots de passe pour l'accès au Fiery server. En outre, EFI recommande à l'administrateur Fiery de modifier le mot de passe par défaut afin de répondre aux exigences de sécurité de l'environnement d'impression de l'utilisateur.

- Le mot de passe autorisé pour « Administrateur » et « Opérateur » peut comporter au maximum 15 caractères lors de l'utilisation de Configure > Sécurité.
- Le mot de passe autorisé pour les comptes d'utilisateurs locaux peut comporter au maximum 64 caractères lors de l'utilisation de Configure > Comptes utilisateur.
- Les mots de passe de l'administrateur et de l'opérateur peuvent également être modifiés dans Configure > Comptes utilisateur lorsque le nombre maximal de caractères autorisés est égal à 64.

Les éléments suivants décrivent les privilèges autorisés pour les différents types d'utilisateurs Fiery :

- **Administrateur** : contrôle complet de toutes les fonctionnalités du Fiery server.

  L'administrateur Fiery peut modifier les droits de tout groupe Fiery, à l'exception des comptes Administrateurs et Opérateurs.
- **Opérateur** : dispose globalement des mêmes droits que l'administrateur, mais n'a pas accès à certaines fonctions du Fiery server, telles que les fonctions de configuration, et ne peut pas supprimer le journal des tâches.
- **Opérateur de presse** (serveurs Fiery XB uniquement) : peut gérer les tâches de la presse. L'administrateur peut ajouter des droits spécifiques à ce type d'utilisateur.
- **Administrateur de service Fiery** (Fiery servers sous Windows seulement) : un compte administrateur caché utilisé pour installer le certificat de confiance sur les serveurs Windows. Ce compte ne permet pas aux utilisateurs de se connecter au Fiery server (local ou distant). Ce compte peut apparaître sur certains outils de numérisation en réseau et peut être supprimé si nécessaire. D'autres méthodes standard peuvent être utilisées pour installer le certificat de confiance.

Journal d'audit de sécurité Fiery

Afin d'aider les organisations à respecter les exigences de conformité, les administrateurs Fiery peuvent collecter et analyser des événements liés à la sécurité, qui sont enregistrés dans le Journal d'audit de sécurité.

Le Journal d'audit de sécurité est activé par défaut.

Chaque événement de sécurité est classifié comme une Information, un Avertissement ou une Erreur. Il n'y a pas d'alertes ou de notifications fournies à l'administrateur, seulement un journal statique.

Les journaux sont dans un format pris en charge par des solutions courantes de collecte et d'analyse de journaux SIEM. Les informations sur les événements capturés sont conformes à la publication spéciale 800-53 du NIST, *Recommended Security Controls for Federal Information Systems* (SP800-53).

L'administrateur Fiery peut lire les événements sans l'intervention d'EFI. Les événements des Fiery servers basés sur Windows et Linux sont au format JSON et peuvent être traités par n'importe quel outil de collecte de journaux. En ce qui concerne les serveurs Fiery basés sur Windows, les événements peuvent être visualisés dans le Gestionnaire d'événements de Windows. Les administrateurs des Fiery servers basés sur Linux peuvent transmettre les journaux vers un système central de collecte de journaux (SysLog).

Les événements de sécurité sont conservés en fonction de la capacité de stockage de disque allouée. Lorsque la taille du journal atteint la limite maximale de stockage (400 Mo), les événements les plus anciens sont supprimés.

Systèmes d'exploitation

EFI collabore étroitement avec les fabricants de systèmes d'exploitation utilisés par les Fiery servers afin d'obtenir les mises à jour de sécurité requises relatives aux problèmes de sécurité et aux vulnérabilités susceptibles d'avoir une incidence sur les composants matériels principaux du Fiery server, tels que la carte mère, le processeur, le BIOS, etc. En outre, les mises à jour logicielles Fiery sont signées numériquement par EFI afin d'éviter toute modification non autorisée, y compris l'insertion de logiciels malveillants.

Linux (FS500)

Les Fiery servers FS500 fonctionnent sous Linux et sont conçus avec une architecture fermée. La visibilité limitée du réseau empêche les accès non autorisés.

Les Fiery servers sous Linux disposent des caractéristiques suivantes :

- Les Fiery servers sous Linux ne comportent pas d'interface locale permettant d'accéder au système d'exploitation.
- Les Fiery servers sous Linux ne prennent pas en charge les protocoles SSH et Telnet, ce qui empêche l'accès à l'interpréteur de commande du système d'exploitation.
- Les Fiery servers sous Linux ne permettent pas l'installation de programmes non autorisés risquant de rendre le système vulnérable.
- Le système d'exploitation Linux utilisé sur les Fiery servers FS500 est un système d'exploitation personnalisé pour les Fiery servers uniquement. Il intègre tous les composants du système d'exploitation requis par un Fiery server, mais pas certains composants d'usage général et certaines applications pour utilisateur final souvent présents dans les systèmes Linux.

Accès au système

Les Fiery servers sous Linux peuvent être configurés à l'aide de la configuration Fiery dans le panneau de commande de l'imprimante ou via Configure dans WebTools. WebTools est un ensemble de pages basées sur navigateur qui permettent à l'administrateur Fiery d'accéder au Fiery server pour la configuration et les autres activités relatives à l'administration du système. WebTools s'exécute dans la dernière infrastructure Web sécurisée prise en charge par la plupart des navigateurs Web modernes.

Windows 10 (FS500 Pro)

Les Fiery servers FS500 Pro autonomes utilisent le système d'exploitation Windows 10 IoT Enterprise 2019 LTSC. Cette version de Windows comprend les tout derniers dispositifs de sécurité ainsi que les améliorations de fonctionnalités cumulatives des versions 1703, 1709, 1803 et 1809 de Windows 10. Chaque build LTSC est prise en charge par Microsoft et dispose de mises à jour de sécurité pendant dix ans après le lancement de la première version.

Remarque : Windows 10 IoT Enterprise 2019 LTSC est un équivalent binaire de Windows 10 Enterprise version 1809.

Windows 10 IoT Enterprise 2019 LTSC comprend les fonctionnalités suivantes :

- Version conçue pour une utilisation sur des systèmes spécialisés tels que les Fiery servers.
- Intègre de nombreuses améliorations sécuritaires de défense contre les menaces, et de protection de l'identité et des informations.
- Fournit de nombreuses mises à jour de sécurité.
- N'inclut pas d'applications orientées au consommateur, comme le Calendrier, la Météo, les Photos, etc.

Microsoft Windows Update

Microsoft publie régulièrement des correctifs de sécurité via Windows Update afin de faire face aux menaces et aux vulnérabilités potentielles de sécurité du système d'exploitation. Windows Update est configuré par défaut sur les Fiery servers pour avertir les utilisateurs lorsque des correctifs sont disponibles, mais sans les télécharger. La sélection de la fonction Rechercher des mises à jour sous Windows Update dans le Panneau de commande de Windows permet d'activer les mises à jour automatiques et de démarrer le processus de mise à jour.

Outils de mise à jour Windows

Les Fiery servers sous Windows utilisent les méthodes Microsoft standard pour mettre à jour tous les correctifs de sécurité Microsoft applicables. Le Fiery server ne prend pas en charge d'autres outils de mise à jour tiers pour la récupération des correctifs de sécurité.

Antivirus Windows

Les Fiery servers sont protégés par les logiciels antivirus Microsoft et Windows 10 Defender. Il est généralement possible d'utiliser des logiciels antivirus tiers sur un Fiery server. Il existe de nombreux logiciels antivirus, qui peuvent inclure un grand nombre de composants et de fonctionnalités conçus pour répondre à une menace particulière.

Veuillez noter qu'un logiciel antivirus est plus efficace lorsqu'il est directement installé, configuré et exécuté sur le Fiery server. Pour les Fiery servers disposant d'une configuration locale, il est possible de lancer un logiciel antivirus sur un PC distant et d'analyser un disque dur partagé du Fiery server. EFI conseille cependant à l'administrateur Fiery de s'adresser directement au fabricant du logiciel antivirus pour bénéficier d'une assistance opérationnelle.

Scan antivirus

Un scan antivirus du Fiery server peut affecter les performances de votre système Fiery, même si le scan est programmé.

Logiciels anti-espions

Un logiciel anti-espion peut affecter les performances du Fiery server lors de la réception de fichiers sur celui-ci. Exemples : tâches d'impression entrantes, fichiers téléchargés lors d'une mise à jour du système du Fiery server ou d'une mise à jour automatique des applications exécutées sur le Fiery server, etc.

Pare-feu intégré
Le Fiery server étant équipé d'un pare-feu, il n'est généralement pas nécessaire de recourir à un pare-feu de logiciel antivirus. EFI recommande aux clients de s'adresser à leur service informatique s'ils ont besoin d'installer et d'exécuter un pare-feu intégré à un logiciel antivirus. Voir Ports réseau à la page 11 la liste des ports disponibles.

Antispam
Le Fiery server prend en charge les fonctions d'impression par e-mail et de numérisation vers e-mail. Nous vous recommandons d'utiliser un mécanisme de filtrage de spam basé sur serveur. Les Fiery servers peuvent également être configurés pour imprimer des documents à partir d'adresses e-mail spécifiées. Le composant antispam n'est pas requis, car il n'est pas possible d'exécuter un client de messagerie distinct (tel qu'Outlook) sur le Fiery server.

Contrôle du HIPS et des applications
Compte tenu de la nature complexe du contrôle du HIPS et des applications, la configuration de l'antivirus doit être testée et rigoureusement validée lors de l'utilisation de l'une ou l'autre de ces fonctionnalités. Avec des paramètres appropriés, le contrôle du HIPS et des applications offre d'excellentes mesures de sécurité qui coexistent parfaitement avec le Fiery server. Cependant, il est très facile de provoquer des problèmes de Fiery server en sélectionnant des paramètres du HIPS ou des exclusions de fichier incorrects, souvent en acceptant simplement les paramètres par défaut. La solution consiste à vérifier les options sélectionnées dans les paramètres de contrôle du HIPS et/ou des applications, ainsi que les paramètres du Fiery server (ports et protocoles réseau, exécutables d'applications, fichiers de configuration, fichiers temporaires, etc.).

Liste autorisée et liste de blocage
Les fonctionnalités de liste autorisée et de liste de blocage n'ont normalement aucune incidence négative sur le Fiery server. EFI conseille vivement à ses clients de configurer ces fonctionnalités afin que les modules Fiery ne soient pas bloqués.

Virus transmis par e-mail

Généralement, l'exécution des virus transmis par e-mail nécessite une action de la part du destinataire. Les fichiers joints qui ne sont pas des fichiers PDL (langage de description de page) sont ignorés par le Fiery server. Le Fiery server ignore également les e-mails au format RTF ou HTML, ainsi que tous les éléments JavaScript inclus. À l'exception des réponses envoyées par e-mail à un utilisateur spécifique en fonction d'une commande reçue, tous les fichiers reçus sont traités comme des tâches PDL.

Remarque : Pour plus d'informations sur le flux de production d'impression par e-mail du Fiery server, voir Impression par e-mail à la page 26.

Sécurité des données

Cette section décrit les contrôles de sécurité conçus pour protéger les données utilisateur résidant dans le Fiery server et les contrôles de sécurité pour les données en transit.

Cryptage des informations essentielles

Le cryptage des informations essentielles dans le Fiery server assure la protection de tous les mots de passe et informations de configuration lorsqu'elles sont stockées dans le Fiery server. Les informations essentielles sont cryptées ou hachées. Les algorithmes de chiffrement utilisés sont AES, Diffie-Hellman et SHA-2 pour se conformer aux dernières normes de sécurité.

Même si le disque est retiré du Fiery server, les informations utilisateur qu'il contient sont illisibles. Le cryptage des données utilisateur peut être activé ou désactivé sur les Fiery servers sous système d'exploitation Windows à l'aide de Configure. Cette fonction est toujours activée pour les Fiery servers sous Linux.

Si la phrase secrète saisie pour récupérer les données est oubliée, il n’est pas possible de la réinitialiser et EFI ne peut pas la récupérer. Le logiciel doit être réinstallé.

Remarque : Avec le cryptage des données, le disque est partitionné et seule la partition de données utilisateur est cryptée. Les partitions du système d’exploitation ne peuvent pas être cryptées.

Norme de cryptage avancé (AES)

Le Fiery server protège les données au repos contre les accès non autorisés. Il crypte les tâches, les images et les données de clients à l’aide de l’algorithme AES 256 bits.

L'AES est une norme de cryptage simple, rapide et difficile à craquer, adaptée à un large éventail d’applications et de périphériques. Il offre un degré de protection supplémentaire contre le vol des données tout en se conformant à la politique de l'entreprise en matière de sécurité.

Impression standard

Les tâches soumises au Fiery server sont envoyées dans l’une des files d'attente d'impression suivantes publiées par le Fiery server :

- Queue Attente
- File d’attente d’impression
- Queue Impression séquentielle
- File d'attente directe (connexion directe)
- Imprimantes virtuelles (files d'attente personnalisées définies par l’administrateur Fiery).

L’administrateur Fiery peut désactiver les files d'attente d'impression et directes pour limiter l’impression automatique.

Queues Attente, Impression et Impression séquentielle

Lorsqu’une tâche est envoyée vers la queue Impression ou la queue Attente, elle est spoulée sur le disque dur du Fiery server. Chaque tâche envoyée vers la queue Attente est conservée sur ce disque dur jusqu’à ce que l’utilisateur la soumette pour impression ou la supprime à l’aide d’un utilitaire de gestion des tâches, tel que la Command WorkStation.

La queue Impression séquentielle permet au Fiery server de conserver l’ordre de certaines tâches envoyées depuis le réseau. Dans le flux de production, ces tâches sont alors traitées dans l’ordre de leur arrivée selon le principe « Première arrivée, première sortie » (FIFO). Lorsque la queue Impression séquentielle est désactivée, les tâches soumises via le Fiery server sont susceptibles d’être imprimées dans le désordre pour de multiples raisons : par exemple, le Fiery server peut permettre aux tâches plus petites de passer en priorité pendant le spoule des tâches plus volumineuses.

Queue Imprimé

Les tâches envoyées à la queue d’impression sont stockées dans la queue Imprimé du Fiery server après l’impression, si cette fonctionnalité est activée. L’administrateur peut définir le nombre de tâches conservées dans cette queue. Lorsque la queue Imprimé est désactivée, les tâches sont automatiquement supprimées une fois l’impression terminée.

File d'attente directe (connexion directe)

La file d'attente directe est conçue pour le téléchargement de polices et les applications qui nécessitent une connexion directe au module PostScript des Fiery servers.

EFI déconseille l’impression vers la file d'attente directe. Le Fiery server supprime toutes les tâches envoyées via la connexion directe une fois l’impression terminée. Cependant, EFI ne garantit pas que tous les fichiers temporaires associés à la tâche seront effacés.

Les tâches composées de fichiers de type VDP (impression de données variables), PDF ou TIFF sont réacheminées vers la file d'attente d'impression lorsqu’elles sont envoyées vers la file d'attente directe. Les tâches envoyées via le service réseau SMB sont susceptibles d’être acheminées vers la file d'attente d'impression lorsqu’elles sont envoyées vers la file d'attente directe.

Suppression d'une tâche

Une tâche ne peut pas être visualisée ni récupérée lorsqu'elle est automatiquement supprimée du Fiery server ou effacée à l’aide des outils Fiery. Si une tâche a été spoulée sur le disque dur du Fiery server, ses éléments peuvent être conservés sur ce disque dur et peuvent théoriquement être récupérés à l’aide de certains outils, tels que des outils d’analyse de disque utilisés dans le domaine légal.

Effacement sécurisé

La fonctionnalité d’effacement sécurisé est conçue pour que, chaque fois qu’une fonction Fiery supprime une tâche reçue, son contenu soit supprimé du disque dur du Fiery server. Lorsqu’une tâche est supprimée, chaque fichier

source de la tâche est remplacé à trois reprises à l'aide d'un algorithme basé sur la méthode d'effacement de données US DoD 5220.22-M.

Flux de production	Effacement sécurisé
Tâches stockées sur le Fiery server ; disque dur ; effacement sécurisé défini sur Activé	Oui
Tâches stockées sur le Fiery server ; disque dur ; effacement sécurisé défini sur Désactivé	Non
Tâches reçues par le Fiery server et supprimées une fois l'effacement sécurisé défini sur Activé	Oui
Tâches reçues par le Fiery server et supprimées avant que l'effacement sécurisé soit défini sur Activé	Non
Copies de tâches envoyées sur un autre Fiery server (équilibrage de la charge)	Non
Tâches archivées sur un support amovible	Non
Tâches archivées sur des disques réseau	Non
Tâches situées sur des périphériques clients	Non
Effacer l'exécution du serveur	Oui
Fusion ou copie de pages dans une autre tâche (par exemple, tâches Fiery Impose ou fichiers PDF combinés)	Non
Tâches reçues à partir de la connexion SMB et enregistrées dans le disque dur du Fiery server	Non
Parties d'une tâche écrite sur le disque dur du Fiery server lors de l'échange du disque ou des opérations de caching (mise en cache) du disque	Non
Entrées du journal des tâches	Non
Entrées du journal des tâches après l'exécution de l'effacement du serveur	Oui
Mise hors tension du Fiery server avant la fin de la suppression de la tâche	Non
Défragmentation du disque dur du Fiery server avant de supprimer la tâche	Non

Remarque : Les plateformes Fiery XB ou les Fiery servers équipés de disques SSD ne prennent pas en charge la fonctionnalité d'effacement sécurisé.

Mémoire système

Le traitement de certains fichiers peut provoquer l'écriture de certaines données de tâches dans la mémoire du système d'exploitation. Dans certains cas, cette mémoire peut être permutée sur le disque dur et peut ne pas être écrasée.

Mémoire volatile			
Type (SRAM, DRAM, etc.)	**Modifiable par l'utilisateur (Oui ou Non)**	**Fonction ou utilisation**	**Traitement d'assainissement**
DRAM	Oui	Mémoire du système principal (reçoit les tâches envoyées à la file d'attente directe)	Mise hors tension du Fiery server
SDRAM (sur la carte vidéo)	Oui	Mémoire vidéo	Mise hors tension du Fiery server

Mémoire non volatile			
Type (SRAM, DRAM, etc.)	**Modifiable par l'utilisateur (Oui ou Non)**	**Fonction ou utilisation**	**Traitement d'assainissement**
BIOS	Non	Fonctions du BIOS	Déconnexion de la fiche et destruction, mais le système cessera de fonctionner.
EPROM Ethernet	Non	Microprogramme de puce Ethernet	Dessoudage et destruction, mais le système cessera de fonctionner.
NVRAM CMOS	Non	Stockage des paramètres du BIOS	Retirer la batterie du système pendant 30 secondes.
Disque dur ou lecteur à circuits intégrés (SSD)	Oui	Système d'exploitation Applications Fiery (disposant potentiellement de données utilisateur) Logiciel système Fiery Tâches d'impression, numérisation de tâches et autres données utilisateur Sauvegarde de l'image pour valeurs d'usine	Réinstallation du logiciel système. La plupart des tâches peuvent être supprimées en toute sécurité grâce à la fonction d'effacement sécurisé*. Il est possible d'utiliser des outils d'assainissement tiers ou développés par des partenaires Fiery en vue de compléter les données d'effacement sur ces périphériques.

Mémoire non volatile			
Type (SRAM, DRAM, etc.)	**Modifiable par l'utilisateur (Oui ou Non)**	**Fonction ou utilisation**	**Traitement d'assainissement**
Remarque : La mémoire volatile et la mémoire vive peuvent contenir des données client lors du traitement des données des clients. Aucune donnée client n'est stockée dans la mémoire non volatile telle que le BIOS, le CMOS ou la NVRAM. *Il est impossible de désinfecter complètement les lecteurs à circuits intégrés par des méthodes de réécriture multi-pass à effacement sécurisé, en raison de l'usure de la mémoire due au mappage. Toute tentative aurait par ailleurs pour effet de réduire considérablement la durée de vie du lecteur SSD. Cette fonctionnalité n'est pas prise en charge par les plates-formes Fiery XB.			

Impression sécurisée

Pour utiliser la fonction d'impression sécurisée, l'utilisateur doit saisir un mot de passe spécifique à la tâche sur le Fiery server et l'imprimante afin que la tâche puisse être imprimée.

Cette fonction nécessite un accès au panneau de commande de l'imprimante. L'objectif de cette fonction est de limiter l'accès à un document à un utilisateur disposant du mot de passe de la tâche et ayant la possibilité de le saisir localement sur le panneau de commande de l'imprimante.

Flux de production d'impression sécurisée

L'utilisateur saisit un mot de passe dans le champ Impression sécurisée du pilote d'impression Fiery. Lorsqu'une tâche est envoyée vers la queue Attente ou Impression du Fiery server, elle est mise en attente jusqu'à la saisie du mot de passe.

Remarque : Les tâches envoyées avec un mot de passe pour l'impression sécurisée ne sont pas visibles à partir de la Command WorkStation.

À partir du panneau de commande de l'imprimante, l'utilisateur accède à la fenêtre Impression sécurisée et saisit son mot de passe. Il peut ensuite localiser les tâches envoyées avec ce mot de passe, les imprimer et/ou les supprimer.

La tâche sécurisée imprimée n'est pas déplacée vers la queue Imprimé et est automatiquement supprimée après l'impression.

Remarque : Une partie des données peut rester temporairement dans les fichiers du système d'exploitation.

Impression par e-mail

Le Fiery server peut recevoir et imprimer des tâches envoyées par e-mail. L'administrateur peut conserver sur le Fiery server, la liste des adresses e-mail autorisées. Tout e-mail reçu depuis une adresse ne figurant pas dans cette liste est supprimé. Par défaut, cette fonctionnalité est désactivée. L'administrateur peut activer et désactiver la fonction d'impression par e-mail.

Gestion des tâches

L'exécution d'actions sur les tâches soumises au Fiery server nécessite un utilitaire Fiery de gestion des tâches avec droits d'accès administrateur ou opérateur.

Journal des tâches

Le journal des tâches est stocké sur le Fiery server. La suppression individuelle des enregistrements est impossible. Le journal contient des informations relatives aux tâches d'impression et de numérisation, telles que le nom de l'utilisateur à l'origine de chaque tâche, l'heure d'exécution, les caractéristiques en termes de papier utilisé, de couleur, etc. Il est possible d'utiliser le journal des tâches pour étudier l'activité du Fiery server.

Un utilisateur disposant de droits d'accès d'opérateur peut afficher, exporter ou imprimer le journal des tâches depuis Fiery Command WorkStation. Un utilisateur possédant des droits d'administrateur peut effacer le journal des tâches depuis Fiery Command WorkStation.

Configuration

Il est impératif de disposer d'un mot de passe administrateur pour réaliser des opérations de configuration. Il est possible de configurer le Fiery server à l'aide de l'outil Configure dans les WebTools ou la Command WorkStation, ou à l'aide de la fonction de configuration du panneau de commande de l'imprimante.

Numérisation

Le Fiery server permet à une image placée sur la vitre de l'imprimante d'être numérisée sur le poste de travail ayant exécuté la demande de numérisation. Lorsqu'une opération de numérisation est exécutée depuis un poste de travail, l'image bitmap brute est directement envoyée à celui-ci.

L'utilisateur peut numériser des documents vers le Fiery server à des fins de distribution, de stockage et de récupération. Tous les documents numérisés sont enregistrés sur le disque. L'administrateur peut configurer le Fiery server de façon à supprimer automatiquement les tâches de numérisation à l'issue d'un délai prédéfini.

Répartition des tâches numérisées

Les tâches de numérisation peuvent être distribuées selon différentes méthodes.

E-mail

Un e-mail contenant une pièce jointe de la tâche numérisée est envoyé à un serveur de messagerie d'où il est acheminé vers la destination souhaitée.

Remarque : Si la taille du fichier est supérieure à la taille maximale définie par l'administrateur, la tâche est stockée sur le disque dur du Fiery server qui est accessible au moyen d'une adresse URL.

FTP

Le fichier est envoyé vers une destination FTP. Un enregistrement du transfert, comprenant la destination, est conservé dans le journal FTP, accessible depuis la commande Imprimer les pages du panneau de commande de l'imprimante. Il est possible de définir un serveur proxy FTP pour envoyer la tâche au travers d'un pare-feu.

Queue Attente du Fiery server

Le fichier est envoyé vers la queue Attente du Fiery server. Il n'est pas conservé en tant que tâche numérisée.

Pour plus d'informations sur la queue Attente du Fiery server, voir Queues Attente, Impression et Impression séquentielle à la page 23.

Fax Internet

Le fichier est envoyé vers un serveur de messagerie, d'où il est acheminé vers la destination fax Internet souhaitée.

Messagerie

Le fichier est stocké sur le Fiery server avec un numéro de messagerie. Pour accéder à la tâche de numérisation stockée, l'utilisateur doit saisir le numéro de messagerie approprié. Les utilisateurs ont la possibilité de définir des mots de passe pour protéger les contenus de leurs boîtes aux lettres de numérisation contre les accès non autorisés. Il est possible de récupérer la tâche de numérisation via une adresse URL.

Conformité aux réglementations et infrastructures

Le tableau ci-dessous présente la conformité aux réglementations et infrastructures pour les serveurs Fiery exécutant le logiciel système FS500 Pro/FS500.

Réglementations / Infrastructures	**Étendue**	**Série NX (FS500 Pro)**	**Série A/E (FS500)**
FIPS 140-2	• Gouvernement américain (fédéral et d'État) • Exigences de sécurité pour les modules de chiffrement	Conformité Windows 10 2019 LTSC Certificats FIPS : • #3197 • #3196 • #3092	Non conformité
Modèles CIS	• Global • Gouvernement / Secteur privé • Lignes de base de la configuration et bonnes pratiques pour la configuration sécurisée d'un système	Conformité Microsoft Windows 10 Entreprise (version 1809)	S/O*
Guide de mise en œuvre technique de sécurité (STIG)	• Norme de configuration du gouvernement (fédérale et d'État) des États-Unis relative aux exigences de cybersécurité pour un produit spécifique	Conformité partielle Windows 10 STIG version 2, R3 Exceptions : ICC-000366 : module de plate-forme fiable (TPM) non disponible	S/O*

Réglementations / Infrastructures	Étendue	Série NX (FS500 Pro)	Série A/E (FS500)
ISO/IEC-15408	• Mondial • Critères communs • Critères d'évaluation des techniques de sécurité informatiques pour la sécurité informatique	Conformité partielle • Authentification LDAP/AD requise pour le contrôle d'accès • TPM et démarrage sécurisé non pris en charge	Non conformité
IEEE 2600.2-2009	• Mondial • Gouvernement / Secteur privé • Profil de critères communs pour les périphériques papier Environnement B	Conformité partielle • TPM et démarrage sécurisé non pris en charge • Les exigences en matière de résistance et de détection nécessitent un kit de sécurité en option pour le disque dur Fiery	Non conformité
Sauvegarde de la matrice d'évaluation de la sécurité informatique (SCSEM)	• Gouvernement américain (fédéral et d'État) • Directives sur la sécurité des informations fiscales pour les organismes fédéraux, nationaux et locaux	Conformité partielle • TPM et démarrage sécurisé non pris en charge • Les exigences en matière de résistance et de détection nécessitent un kit de sécurité en option pour le disque dur Fiery	Non conformité
DoD 522.22-M	Norme d'assainissement des données. 3 passages	Conformité	Conformité
NIST 800-88	Norme d'assainissement des données. 1 passage	Non conformité	Non conformité
Certification dans le cadre de gestion des risques de l'armée (RMF)	• Gouvernement américain • Cadre de gestion des risques pour la technologie de l'information militaire	Conformité partielle • TPM et démarrage sécurisé non pris en charge	Conformité partielle • TPM et démarrage sécurisé non pris en charge

*Hors du champ d'application de la réglementation ou du cadre. Les serveurs sous Linux série E et A sont des systèmes fermés, sans accès direct au système de fichiers. La visibilité limitée du réseau empêche les accès non autorisés.

Conformité FIPS 140-2

Lorsqu'ils sont configurés correctement, les serveurs Fiery qui exécutent FS500 Pro sous Windows 10 2019 LTSC sont conformes aux instructions de chiffrement des données FIPS 140-2. Un serveur Fiery mis en *mode FIPS 140-2* utilise uniquement des algorithmes de chiffrement validés et certifiés via le programme Cryptographic Algorithm Validation Program (CAVP) du gouvernement fédéral des États-Unis pour le chiffrement des données au repos et en transit.

L'activation du *mode FIPS 140-2* dans Fiery nécessite que l'utilisateur suive un processus de configuration avancé pour renforcer le serveur.

Directives pour une configuration du serveur Fiery sécurisée

Les instructions suivantes peuvent aider les administrateurs Fiery à améliorer la sécurité lors de la configuration du Fiery server.

Modification du mot de passe administrateur

Nous vous recommandons de modifier le mot de passe par défaut de l'administrateur Fiery lors de l'installation et à intervalles réguliers, conformément aux stratégies de sécurité de votre entreprise. Les mots de passe par défaut de l'administrateur doivent être modifiés dans l'Assistant de configuration du Fiery lors de la première configuration. Les mots de passe de l'administrateur et de l'opérateur peuvent être modifiés après la première configuration dans les WebTools : Configure > Sécurité > Mot de passe administrateur (ou opérateur, respectivement). La configuration des mots de passe est également disponible à partir des Comptes utilisateur.

Le mot de passe administrateur offre à l'utilisateur un accès total au Fiery server localement et/ou depuis un ordinateur distant. L'accès complet comprend, mais sans s'y limiter :

- Système de fichiers
- Stratégie de sécurité du système
- Entrées de registre
- Mot de passe administrateur, refusant aux utilisateurs anonymes l'accès au Fiery server

Paramètres conseillés

- Choisissez le niveau de sécurité maximal pour le protocole SNMP dans Réseau > SNMP :

  Le choix de la sécurité maximale limite la prise en charge du protocole SNMP v3 uniquement sur le Fiery server.

  Si le gestionnaire SNMP fonctionne uniquement avec le protocole SNMP v1/v2c, modifiez la valeur du champ Nom de communauté en lecture. Le Fiery server vous permet de modifier les valeurs des champs SNMP Nom de communauté en lecture et Nom de communauté en écriture à partir des WebTools (Configure > Réseau > SNMP) et du panneau de commande de l'imprimante (Réseau > SNMP).
- Désactivez WSD dans la soumission des tâches.
- Désactivez l'impression Windows dans la soumission des tâches si vous utilisez LPR, port 9100 ou IPP pour imprimer.
- Bloquez les ports en activant le filtre de port TCP/IP dans le filtrage de port Sécurité > TCP/IP.

  Désactivez les ports 137-139 et 445 si vous n'utilisez pas l'impression Windows et que vous n'avez pas besoin d'accéder aux fichiers ou de partager ces dossiers. Désactivez les communications non sécurisées sur le port 80 (HTTP).

Outre les protections au niveau du système d'exploitation, le Fiery server dispose des fonctions de sécurité supplémentaires suivantes pour protéger vos données :

- Les Fiery servers sont dotés de l'impression sécurisée pour veiller à ce que l'utilisateur récupère uniquement ses tâches d'impression.
- Les Fiery servers s'intègrent aux principales solutions comptables pour offrir davantage de sécurité via l'impression Follow-me.

Les Fiery servers comportent de nombreuses fonctionnalités de sécurité, mais ne sont pas des serveurs orientés Internet. Ils doivent être installés dans un environnement protégé et leur accessibilité doit être configurée correctement par l'administrateur réseau.

Sélectionner un profil de sécurité Élevé

Le Fiery server offre des recommandations de sécurité prédéfinies en fonction du niveau de risques et de menaces (Standard, Élevé, Courant). Cette fonctionnalité est appelée Profils de sécurité. Elle est accessible à partir des emplacements suivants :

- Assistant logiciel Fiery
- WebTools > Configure > Sécurité

Le profil de sécurité Élevé permet de renforcer la sécurité du Fiery server et active les fonctionnalités de sécurité les plus couramment utilisées.

Option	Élevée
Filtrage du port TCP/IP	Activé
Protocole SLP (Service Location Protocol)	Désactivé
Bonjour	Désactivé
Effacement sécurisé	Activé
Bureau à distance	Désactivé
Mot de passe SMB	Activé
Périphériques de stockage USB	Désactivés
Sécurité PostScript	Activée
Port 9100	Désactivé
LPD	Activé
Impression Windows	Désactivée
IPP	Activée
Services Web pour périphériques (WSD)	Désactivés
Impression par e-mail	Désactivée

Option	Élevée
Impression FTP	Désactivée
Impression mobile directe	Désactivée

EFI recommande d'utiliser le profil de sécurité Élevé pour les environnements présentant des exigences de sécurité maximales.

Conclusion

Avec le Fiery Server, EFI offre un ensemble performant de fonctionnalités de sécurité standard et optionnelles sur le Fiery server pour offrir à nos clients des solutions de sécurité complètes et personnalisables, adaptées à tous les environnements. EFI s'engage à veiller à ce que le Fiery server soit efficacement protégé contre toute vulnérabilité à une utilisation malveillante ou non intentionnelle afin que nos clients puissent exploiter leurs entreprises à un rendement maximal.