Livre blanc sur la sécurité du système Fiery

Fiery FS200/FS200 Pro Servers

Date de publication : Mai 2018

Livres blancs

Livre blanc sur la sécurité du système Fiery

Table des matières

1 Aperçu du document

Ce document présente l'architecture du Fiery ® Server et les aspects fonctionnels associés à la sécurité des périphériques dans les Fiery FS200/FS200 Pro Servers. Il traite de la sécurité matérielle et du réseau, du contrôle d'accès, ainsi que de la sécurité du système d'exploitation et des données.

Ce document a pour objet d'aider les utilisateurs à comprendre toutes les fonctionnalités de sécurité du Fiery Server dont ils peuvent bénéficier et à identifier les vulnérabilités potentielles.

1.1 Philosophie de sécurité d'EFI

EFI™ a conscience que la sécurité constitue aujourd'hui une préoccupation essentielle pour les entreprises du monde entier. C'est pourquoi les Fiery Servers intègrent de puissantes fonctionnalités de sécurité conçues pour protéger leurs ressources les plus précieuses.
Nous collaborons également de manière proactive avec nos partenaires OEM internationaux et nos équipes interfonctionnelles afin de déterminer les exigences actuelles et futures des entreprises en matière de sécurité, de façon que nos produits ne posent aucun problème de sécurité.
Comme d'ordinaire, nous recommandons cependant aux utilisateurs de combiner les fonctionnalités de sécurité du Fiery Server avec d'autres mesures de protection, telles que des mots de passe sécurisés et des procédures de sécurité physique rigoureuses, pour garantir la sécurité globale du système.

1.2 Configuration des fonctionnalités de sécurité via Fiery Configure

Les utilisateurs accédant au Fiery Server depuis la Fiery Command WorkStation® à l'aide d'un compte administrateur peuvent configurer toutes les fonctionnalités de sécurité via Fiery Configure. Il est possible de lancer Fiery Configure depuis la Fiery Command WorkStation ou les WebTools™, dans l'onglet Configurer.

2 Sécurité matérielle et physique

2.1 Mémoire volatile

Le Fiery Server utilise une mémoire RAM volatile pour la mémoire locale du processeur et pour la mémoire de travail requise pour le système d'exploitation, le logiciel du système Fiery et les données d'image. Les données écrites dans la mémoire RAM sont conservées tant que le système est sous tension. Lorsqu'il est mis hors tension, toutes les données sont supprimées.

2.2 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 système est mis hors tension. Ces données se composent d'informations de programmation du système et de données d'utilisateur.

2.2.1 Mémoire flash

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

Une partie de la mémoire flash est également utilisée pour consigner l'utilisation de clés électroniques afin d'activer des options logicielles Fiery.

Aucune donnée d'utilisateur n'est stockée sur ce dispositif et l'utilisateur n'a pas accès aux données qu'il contient.

2.2.2 Mémoire CMOS

Disposant d'une batterie de sauvegarde, la mémoire CMOS permet de stocker les paramètres système du serveur. Ces informations ne sont pas considérées comme étant confidentielles ou privées. Les utilisateurs peuvent accéder à ces paramètres sur un serveur Windows 8.1 Pro via Fiery Integrated Workstation (kit FACI incluant souris, clavier et moniteur locaux) si ce kit est installé.

2.2.3 Mémoire 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.

2.2.4 Disque dur

Lors des opérations normales d'impression et de numérisation, et de la création des informations de gestion des tâches, des données d'image sont écrites dans une zone aléatoire du disque dur.

Les données d'image et les informations de gestion des tâches peuvent être supprimées par un opérateur ou à l'expiration d'un délai prédéfini. Les données d'image deviennent alors inaccessibles.

Pour protéger les données d'image contre tout accès non autorisé, EFI propose une fonctionnalité d'effacement sécurisé (voir la section 6.2.5). Une fois cette fonctionnalité activée par l'administrateur système, l'opération sélectionnée est exécutée au moment approprié afin d'effacer de façon sécurisée les données supprimées du disque dur.

2.2.5 Ports physiques

Il est possible de connecter le Fiery Server par l'intermédiaire des ports externes suivants :

Ports Fiery	Fonction	Accès	Contrôle d'accès
Connecteur Ethernet RJ-45	Connectivité Ethernet	Connexions réseau (voir les connexions d'impression et de réseau ci-dessous)	Utilisation du filtrage IP Fiery pour contrôler l'accès
Connecteur d'interface du copieur	Impression/ numérisation	Dédié à l'envoi/ la réception de données vers/depuis l'imprimante	Non applicable
Port USB	Connexion de périphériques USB	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.

2.3 Interface locale

L'utilisateur peut accéder aux fonctions du système Fiery via le kit FACI (s'il est activé sur un serveur Windows 8.1 Pro) ou depuis l'écran LCD Fiery sur les Fiery Servers. Sur un Fiery Server équipé du kit FACI, l'accès aux fonctions de sécurité est contrôlé au moyen du mot de passe administrateur Windows si le kit FACI est activé. L'écran LCD Fiery permet d'accéder à des fonctions très limitées qui ne génèrent aucun risque de sécurité.

2.4 Kit de disque dur extractible en option

Le Fiery Server prend en charge, en option, un kit de disque dur extractible pour 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 serveur mis hors tension.

2.4.1 Pour serveurs externes

Les Fiery Servers prennent en charge un kit de disque dur extractible en option. La disponibilité de ce kit pour un produit Fiery spécifique dépend des termes des accords de développement et de distribution conclus par EFI avec chacun de ses partenaires OEM.

2.4.2 Pour serveurs intégrés

Pour les produits intégrés, le disque dur extractible est disponible uniquement sous la forme d'une option proposée en coordination avec chaque partenaire OEM, car l'emplacement et les supports de montage dans l'imprimante multifonction doivent être développés conjointement avec le partenaire OEM. Le kit en option implique d'extraire le disque dur interne du châssis intégré et de l'installer dans un boîtier externe disposant d'une alimentation distincte.

3 Sécurité du réseau

Les fonctionnalités standard de sécurité réseau du Fiery Server offrent la possibilité de laisser uniquement les utilisateurs et groupes autorisés accéder au périphérique de sortie et imprimer des documents sur celui-ci, de limiter les communications du périphérique aux adresses IP spécifiées et de contrôler la disponibilité des protocoles et ports réseau individuels, comme souhaité.

Bien que le Fiery Server intègre de nombreuses fonctionnalités de sécurité, il ne s'agit pas d'un serveur avec accès via Internet. Il doit être déployé dans un environnement protégé et son accessibilité configurée correctement par l'administrateur réseau.

3.1 Ports réseau

Le Fiery Server permet à l'administrateur réseau d'activer et de désactiver les ports IP suivants de manière sélective. Il est ainsi possible de bloquer efficacement les communications avec des périphériques indésirables et l'accès au système via des protocoles de transport spécifiques.

TCP	UDP	Nom du port	Services associés
20–21		FTP	
80		HTTP	WebTools, IPP
135		MS RPC	Service RPC Microsoft® (Windows 8.1 Pro 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	WebTools, Fiery Central, certains utilitaires plus anciens, autres outils SNMP
	427	SLP	
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB sur TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impression LPR, certains utilitaires plus anciens (tels que les WebTools et les versions antérieures de la CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPsec
	5353	DNS multidiffusion	Bonjour
3389		RDP	Remote Desktop (Windows Fiery servers only)
3702	3702	WS-Discovery	WSD
6310 8010 8021–8022 8090 9906 18021 18022 18081 18082 21030 22000 50006 - 50025*	9906	Ports EFI	Command WorkStation 4 et 5, Fiery Central, outils SDK (kit de développement logiciel) d'EFI, fonctions bidirectionnelles du pilote d'imprimante Fiery, WebTools, Fiery Direct Mobile Printing et conversion de documents natifs
9100–9103		Port d'impression	Port 9100

Les autres ports TCP sont désactivés, à l'exception de ceux spécifiés par le partenaire OEM. 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.

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

3.2 Filtrage IP

L'administrateur peut limiter les connexions autorisées avec le Fiery Server aux hôtes dont les adresses IP appartiennent à une plage IP particulière. Les commandes ou les tâches provenant d'adresses IP non autorisées sont ignorées par le Fiery Server.

3.3 Chiffrement réseau

3.3.1 IPsec

IPsec (*Internet Protocol security*) assure la sécurité de toutes les applications sur les protocoles IP par le chiffrement 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.

* Ces ports sont actifs à condition que Fiery Command WorkStation version 6.2 ou ultérieure soit installé sur un serveur Fiery externe.

3.3.2 SSL et TLS

Les protocoles SSL/TLS sont des protocoles de niveau application utilisés pour transmettre des messages sur Internet de façon sécurisée. Les Fiery Servers prennent en charge les protocoles SSL v2/v3 et TLS v1.

Plusieurs fonctionnalités des Fiery Servers prennent en charge les protocoles SSL/TLS. Les utilisateurs peuvent accéder à la page d'accueil et aux API Web du Fiery Server de façon sécurisée au moyen de ces protocoles. Il est également possible de les sélectionner pour la connexion aux serveurs LDAP et aux serveurs de messagerie électronique afin de garantir des communications sécurisées.

3.3.3 Gestion des certificats

Les Fiery Servers offrent une interface dédiée à la gestion des certificats utilisés pour les différentes communications SSL/TLS. Celle-ci prend en charge le format de certificat X.509.

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'un magasin de certificats approuvé.

3.4 IEEE 802.1x

La norme 802.1x est un protocole IEEE standard pour le contrôle d'accès au réseau basé sur des ports. Ce protocole assure l'authentification des périphériques avant qu'ils accèdent 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 ou PEAP-MSCHAPv2 pour l'authentification sur un serveur d'authentification 802.1x.

Le Fiery Server s'authentifie au démarrage ou lorsque le câble Ethernet est déconnecté, puis reconnecté.

3.5 SNMP v3

Le Fiery Server prend en charge le protocole SNMPv3, qui est un protocole réseau sécurisé pour la gestion de périphériques sur des réseaux IP. Les paquets de communication SNMPv3 peuvent être chiffrés pour veiller à leur confidentialité. L'intégrité et l'authentification des messages est également assurée.

L'administrateur Fiery a la possibilité de sélectionner l'un des trois niveaux de sécurité disponibles pour le protocole SNMPv3. Il peut également exiger une authentification avant d'autoriser les transactions SNMP et chiffrer les noms d'utilisateur et mots de passe SNMP.

3.6 Sécurité des e-mails

Le Fiery Server prend en charge les protocoles POP et SMTP. Pour protéger le service contre les risques d'attaque et d'utilisation inappropriée, l'administrateur Fiery peut activer des fonctionnalités de sécurité additionnelles, comme détaillé ci-dessous :

3.6.1 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 de messagerie 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.

3.6.2 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.

4 Contrôle d'accès

4.1 Authentification des utilisateurs

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

- authentifier les noms d'utilisateur ;
- autoriser des actions en fonction des droits de l'utilisateur.

Le Fiery Server peut authentifier des 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 N&B, Imprimer en couleur et en N&B) et les actions des membres du groupe sont limitées à ces droits.

Les groupes Fiery sont des groupes d'utilisateurs disposant d'un ensemble de droits prédéfinis. Un groupe Fiery accorde certains droits à des utilisateurs.

L'administrateur Fiery peut modifier les droits de tout groupe Fiery, à l'exception des utilisateurs administrateurs, opérateurs et invités.

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

- Imprimer en N&B : ce droit permet aux membres d'un groupe d'imprimer des tâches sur le Fiery Server. Si l'utilisateur ne dispose pas du droit Imprimer en couleur et en N&B, le Fiery Server force l'impression de la tâche en noir et blanc.
- Imprimer en couleur et en N&B : ce droit permet aux membres d'un groupe d'imprimer des tâches sur le Fiery Server avec un accès total aux capacités d'impression en couleur et en niveaux de gris. Si l'utilisateur ne dispose pas de ce droit ou du droit Imprimer en N&B, l'impression de la tâche est impossible et l'utilisateur ne peut pas soumettre la tâche via FTP (périphériques couleur uniquement).
- Boîte Fiery : ce droit permet aux membres d'un groupe de disposer de boîtes individuelles. Le Fiery Server crée une boîte en fonction du nom d'utilisateur associé à ce droit. L'accès à cette boîte s'effectue uniquement à l'aide du nom d'utilisateur/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 de tâche couramment utilisés.
- Gérer des flux de production : ce droit permet aux membres d'un groupe de créer, publier ou modifier des imprimantes virtuelles.

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

4.2 Authentification logicielle Fiery

Le Fiery Server définit des utilisateurs administrateurs, opérateurs et invités, qui disposent de droits différents. 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 de remplacer le mot de passe par défaut par un autre mot de passe, conforme aux critères de sécurité de l'utilisateur final.

Les trois niveaux de mots de passe du Fiery Server permettent d'accéder aux droits suivants :

- Administrateur : bénéficie d'un contrôle total sur toutes les fonctionnalités du Fiery Server.
- Opérateur : dispose globalement des mêmes droits que l'administrateur, mais n'a pas accès à certaines fonctions du serveur, telles que les fonctions de configuration, et ne peut pas effacer le journal des tâches.
- Invité (par défaut, aucun mot de passe) : dispose globalement des mêmes droits que l'opérateur, mais ne peut pas accéder au journal des tâches, apporter des modifications aux tâches d'impression ou changer leur statut, ni prévisualiser les tâches.

5 Environnement du système d'exploitation

5.1 Procédures de démarrage

Le système d'exploitation et le logiciel du système Fiery sont chargés depuis le disque dur local lors du démarrage.

Le BIOS résidant de la carte mère Fiery est accessible en lecture seule et stocke les informations nécessaires à l'amorçage du système d'exploitation. Toute modification ou suppression du BIOS empêche le Fiery Server de fonctionner correctement.

La page de configuration répertorie les valeurs spécifiées durant la configuration. Certaines informations, telles que celles relatives au proxy FTP, aux mots de passe et aux noms de communautés SNMP, ne sont pas indiquées sur cette page.

5.2 Linux

Les systèmes Linux ne comportent pas d'interface locale permettant d'accéder au système d'exploitation.

5.2.1 Logiciel antivirus Linux

Le système d'exploitation Linux utilisé sur les Fiery Servers est un système d'exploitation dédié uniquement à ces serveurs. Il comporte tous les composants requis par un Fiery Server, mais n'intègre pas certains composants à usage général pour les systèmes Linux, tels qu'Ubuntu. En plus d'offrir des performances accrues, ce système d'exploitation dédié ne présente pas les mêmes vulnérabilités aux virus que les systèmes Linux et systèmes d'exploitation Microsoft à usage général. Il est possible que le logiciel antivirus conçu pour les systèmes d'exploitation Linux à usage général ne fonctionne pas sur les Fiery Servers.

5.3 Windows 8.1 Pro

Le Fiery Server est fourni avec un mot de passe administrateur Windows 8.1 par défaut. Il est conseillé à l'administrateur de modifier ce mot de passe lors de l'installation.
Il est également fortement recommandé de le modifier régulièrement afin de se conformer à la politique de sécurité informatique de l'entreprise. Le mot de passe administrateur offre à un utilisateur un accès total au Fiery Server localement et/ou depuis un poste de travail distant, notamment, mais sans s'y limiter, au système de fichiers, à la politique de sécurité du système et aux entrées de registre. Par ailleurs, cet utilisateur peut modifier le mot de passe administrateur et refuser l'accès de tout autre utilisateur au Fiery Server.

5.3.1 Correctifs de sécurité Microsoft

Microsoft publie régulièrement des correctifs de sécurité pour résoudre des failles potentielles de sécurité dans le système d'exploitation Windows 8.1. Windows Update est configuré par défaut pour avertir les utilisateurs lorsque des correctifs sont disponibles, mais sans les télécharger. L'administrateur Fiery peut modifier le paramètre par défaut de Windows Update ou installer manuellement les correctifs de sécurité.

5.3.2 Outils SMS

EFI possède son propre outil dédié de mise à jour pour ses systèmes basés sur Windows. Cet outil gère la récupération de tous les correctifs de sécurité Microsoft et de toutes les mises à jour logicielles Fiery applicables. Le Fiery Server ne prend en charge aucun outil SMS tiers pour la récupération et l'installation de mises à jour sur le Fiery Server.

5.3.3 Logiciel antivirus Windows

Généralement, il est possible d'utiliser un logiciel antivirus avec 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. Cette section présente quelques conseils pour aider les clients à choisir leur logiciel antivirus en toute confiance. Les logiciels de protection contre les virus sont surtout utiles dans une configuration de kit FACI local, où les utilisateurs sont susceptibles d'infecter le Fiery Server par des actions standard effectuées via Windows. Pour les Fiery Servers non équipés du kit FACI, il est possible de lancer un logiciel antivirus sur un PC distant et d'analyser un disque dur partagé du Fiery Server. Cependant, EFI conseille à l'administrateur Fiery de s'adresser directement à l'éditeur du logiciel antivirus pour bénéficier d'une assistance opérationnelle. Voici les recommandations d'EFI pour chacun des composants du logiciel antivirus Windows :

Moteur antivirus : l'analyse (programmée ou non) du Fiery Server par un moteur antivirus peut affecter les performances du serveur.

Logiciel anti-espion : un logiciel anti-espion peut affecter les performances du Fiery Server lors de l'arrivée de fichiers sur celui-ci (tâches d'impression entrantes, fichiers téléchargés pendant une mise à jour du système Fiery ou 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 et de se reporter à la section 3.1 de ce document s'ils ont besoin d'installer et d'exécuter un pare-feu intégré à un logiciel antivirus.

Antispam : le système Fiery prend en charge les fonctionnalités d'impression par e-mail et de numérisation vers un e-mail. Nous recommandons l'utilisation d'un dispositif de filtrage antispam sur le serveur. Les Fiery Servers peuvent également être configurés pour imprimer des documents à partir d'adresses e-mail définies. 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.

Liste blanche et liste noire : ces fonctionnalités n'ont normalement aucune incidence sur le Fiery Server. EFI recommande vivement aux clients de configurer les paramètres de sorte que les modules Fiery ne soient pas placés sur liste noire.

Contrôle des périphériques d'interface utilisateur (HID) et des applications : compte tenu de la nature complexe du contrôle des HID 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 des HID 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 serveur en sélectionnant des paramètres de HID 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 des HID et/ou des applications, ainsi que les paramètres du Fiery Server (ports et protocoles réseau, exécutables d'applications, fichiers de configuration, fichiers temporaires, etc.).

5.4 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. Reportez-vous à la section 6.4 de ce document pour obtenir des informations sur le flux d'impression par e-mail du système Fiery.

6 Sécurité des données

6.1 Chiffrement des informations essentielles

Le chiffrement des informations essentielles assure la protection de tous les mots de passe et de toutes les informations de configuration associées stockés sur le Fiery Server. Pour ce faire, des algorithmes de chiffrement conformes aux normes NIST 2010 sont utilisés.

6.2 Impression standard

Les tâches soumises au Fiery Server sont envoyées dans l'une des queues suivantes publiées par le Fiery Server :

- Queue Attente ;
- Queue Impression ;
- Queue Impression séquentielle ;
- Queue Direct (connexion directe) ;
- Imprimantes virtuelles (queues personnalisées définies par l'administrateur Fiery).

L'administrateur Fiery peut désactiver les queues Impression et Direct pour limiter l'impression automatique. Grâce à des mots de passe activés sur le Fiery Server, cette fonctionnalité restreint la possibilité de réaliser des impressions aux opérateurs et aux administrateurs Fiery.

6.2.1 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 Fiery Command WorkStation, la Fiery Command WorkStation ME ou Effacer le serveur.

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

6.2.2 Queue Imprimé

Les tâches envoyées à la queue Impression sont stockées dans la queue Imprimé, sur le Fiery Server, si celle-ci est activée. L'administrateur peut définir le nombre de tâches conservées dans cette queue. Lorsqu'elle est désactivée, les tâches sont automatiquement supprimées une fois l'impression terminée.

6.2.3 Queue Direct (connexion directe)

La queue Direct est conçue pour le téléchargement de polices et les applications qui nécessitent une connexion directe au module PostScript des contrôleurs Fiery.

EFI déconseille l'impression vers la queue Direct. Le système Fiery 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, PDF ou TIFF sont réacheminées vers la queue Impression lorsqu'elles sont envoyées vers la queue Direct. Les tâches envoyées via le service réseau SMB sont susceptible d'être acheminées vers la queue Impression lorsqu'elles sont envoyées vers la queue Direct.

6.2.4 Suppression de tâches

Les tâches supprimées du Fiery Server, soit automatiquement soit en utilisant des outils Fiery, ne peuvent pas être visualisées ou récupérées à l'aide d'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 judiciaire.

6.2.5 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. À la suppression, le fichier source de chaque tâche est écrasé trois fois à l'aide d'un algorithme basé sur la spécification DoD5220.22M du département de la Défense des États-Unis.

L'effacement sécurisé est soumis aux limitations et restrictions suivantes :

- Il ne s'applique pas aux fichiers de tâches qui se trouvent sur des systèmes autres que le Fiery Server, tels que :
  – les copies de la tâche réparties sur un autre Fiery Server (équilibrage de la charge) ;
  – les copies de la tâche archivées sur des supports ou des lecteurs réseau ;
  – les copies de la tâche stockées sur des postes de travail clients ;
  – les pages d'une tâche fusionnées ou copiées entièrement dans une autre tâche.
- Il ne permet d'effacer aucune entrée du journal des tâches.
- Si le système est mis hors tension manuellement avant la fin de la suppression d'une tâche, rien ne garantit que la tâche sera entièrement effacée.
- Il ne permet pas d'effacer les données de tâche ayant pu être écrites sur disque en raison d'une opération de swapping ou de mise en cache de disque.
- Les tâches soumises via un serveur FTP peuvent être enregistrées par le client FTP avant d'être transmises au logiciel du système Fiery. Le logiciel du système Fiery n'exerçant aucun contrôle sur ce processus, le système ne peut pas effacer de façon sécurisée les tâches enregistrées par le client FTP.
- Les tâches imprimées via SMB sont acheminées par l'intermédiaire du spouleur du Fiery Server, qui les enregistre sur le disque. Le logiciel du système Fiery n'exerçant aucun contrôle sur ce processus, le système ne peut pas effacer ces tâches de façon sécurisée.

Remarque : le swapping (permutation) sert à créer une mémoire virtuelle supérieure à la mémoire physique disponible. Ce processus est exécuté sur la couche du système d'exploitation sans être contrôlé par le Fiery Server. Cependant, des données sont régulièrement réécrites dans l'espace de permutation de disque durant le fonctionnement du système d'exploitation, car de nombreux segments de mémoire sont déplacés entre la mémoire et le disque. En raison de ce processus, certains segments de tâches peuvent être temporairement stockés sur le disque.

6.2.6 Mémoire du 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 mise en cache sur le disque dur et n'est pas spécifiquement écrasée.

6.3 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, afin que celle-ci puisse être imprimée. Cette fonctionnalité nécessite une interface LCD locale sur le Fiery Server.

Cette fonctionnalité a pour objet de limiter l'accès à un document à un utilisateur qui a) dispose du mot de passe associé à la tâche et b) peut le saisir localement sur le Fiery Server.

6.3.1 Flux de production

L'utilisateur saisit un mot de passe dans le champ Impression sécurisée du pilote d'impression Fiery Driver. 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 d'impression sécurisée ne peuvent pas être visualisées depuis la Fiery Command WorkStation ou la Fiery Command WorkStation ME.

A partir de l'écran LCD du Fiery Server, l'utilisateur accède à la fenêtre Impression sécurisée et saisit un mot de passe. Il peut ensuite accéder aux tâches envoyées avec ce mot de passe et les imprimer et/ou les supprimer.

Une fois imprimée, la tâche d'impression n'est pas placée dans la queue Imprimé. Elle est automatiquement supprimée.

6.4 Impression par e-mail

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

6.5 Gestion des tâches

Les tâches envoyées au Fiery Server peuvent être traitées uniquement à l'aide d'un utilitaire de gestion des tâches Fiery, avec des droits d'accès d'administrateur ou d'opérateur. Les utilisateurs invités (qui ne disposent pas d'un mot de passe) peuvent consulter les noms de fichiers et les attributs des tâches, mais ne peuvent réaliser aucune opération ni prévisualiser ces tâches.

6.6 Journal des tâches

Le journal des tâches est stocké sur le Fiery Server. Il est impossible d'y supprimer individuellement des enregistrements. 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, la date et 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 la Fiery Command WorkStation. Un utilisateur possédant des droits d'administrateur peut effacer le journal des tâches depuis la Fiery Command WorkStation. Un utilisateur invité peut imprimer le journal des tâches depuis l'écran LCD du système Fiery et ce, uniquement si cet accès lui est accordé par l'administrateur.

6.7 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 depuis l'outil Fiery Configure ou depuis le menu Configuration disponible sur l'écran LCD du système Fiery. L'outil Fiery Configure peut être lancé depuis les Fiery WebTools et depuis la Fiery Command WorkStation.

6.8 Numérisation

Grâce au Fiery Server, il est possible de numériser une image placée sur la vitre d'exposition du copieur et de l'envoyer au poste de travail à l'origine de cette opération de numérisation, à l'aide d'un module externe TWAIN Fiery. Ce module est pris en charge par les applications Adobe® PhotoShop et Textbridge. 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.

Il est possible de distribuer les tâches de numérisation par les méthodes suivantes :

- E-mail : dans le cadre de ce processus, un e-mail 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 maximum 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 le menu Imprimer les pages de l'écran LCD. Il est possible de définir un serveur proxy FTP pour envoyer la tâche au travers d'un pare-feu.
- Queue Attente Fiery : le fichier est envoyé vers la queue Attente du Fiery Server (voir la section 6.2.1 ci-dessus) et n'est pas conservé en tant que tâche de numérisation.
- Fax Internet : le fichier est envoyé à un serveur de messagerie, d'où il est acheminé vers la destination fax Internet souhaitée.
- Boîte : le fichier est stocké sur le Fiery Server avec un numéro de boîte. Pour accéder à la tâche de numérisation stockée, l'utilisateur doit saisir le numéro de boîte approprié. Certaines versions du Fiery Server exigent également un mot de passe. Il est possible de récupérer la tâche de numérisation via une adresse URL.

7 Conclusion

Avec le Fiery Server, EFI offre un ensemble performant de fonctionnalités standard et optionnelles pour répondre aux besoins de ses clients en leur permettant de bénéficier d'une solution de sécurité complète et personnalisable, adaptée à tous les environnements. EFI s'emploie à optimiser au maximum les activités de ses clients et à protéger efficacement le Fiery Server déployé contre toutes les vulnérabilités découlant d'une utilisation malveillante ou accidentelle.
C'est pourquoi EFI développe constamment de nouvelles technologies pour offrir des solutions de sécurité exhaustives et extrêmement fiables pour le Fiery Server.

TL035.07.18_FR