Fiery FS700 Pro/FS700 servers

Security White Paper

45266126

8 décembre 2025

Sommaire

Présentation

Ce document présente les fonctionnalités de sécurité des serveurs Fiery. Il vise à informer les administrateurs informatiques et les professionnels de la sécurité sur la manière dont les solutions Fiery sécurisent les environnements d'impression sécurisée. Ce document explique les principes et les mécanismes utilisés par les serveurs Fiery pour protéger les données, renforcer la sécurité du réseau et préserver l'intégrité du système.

Principes de sécurité

Fiery servers sont méticuleusement conçus pour adhérer aux meilleures pratiques de l'industrie, garantissant la conformité aux réglementations en matière de protection des données et aux exigences de sécurité de l'entreprise. Les principes fondamentaux qui sous-tendent cette conception sont les suivants :

- Protection des données : chiffrement des données au repos et des données en transit
- Sécurité du réseau : accès contrôlé, protocoles de communication sécurisés et mécanismes d'authentification
- Intégrité du système : vérification du micrologiciel, démarrage sécurisé et mises à jour de sécurité

En collaboration avec nos partenaires et fournisseurs mondiaux, nous fournissons un soutien continu à nos clients à mesure que les menaces évoluent. Afin de garantir une sécurité complète du système, nous recommandons aux utilisateurs finaux d'intégrer les fonctionnalités de sécurité Fiery aux stratégies de sécurité de leur propre entreprise et de respecter les meilleures pratiques du secteur, notamment la mise en œuvre de mots de passe sécurisés et de mesures de sécurité physique robustes.

Authentification et contrôle d'accès

Les serveurs Fiery prennent en charge plusieurs méthodes d'authentification, notamment :

- Contrôle d'accès basé sur les rôles (RBAC)
- Intégration LDAP/Active Directory
- Authentification multifacteur (MFA) implémentée via la connexion unique (SSO)

Authentification utilisateur

La fonctionnalité d'authentification permet au serveur Fiery d'exécuter les fonctions suivantes :

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

Le Fiery server prend en charge trois méthodes d'authentification :

- Authentification locale pour les utilisateurs définis sur le serveur Fiery
- Authentification à facteur unique (SFA) via des serveurs d'authentification réseau externes en utilisant LDAP (par exemple, Microsoft Active Directory)
- Authentification multifacteur (MFA) à l'aide de la connexion unique (SSO)

Quelle que soit la méthode utilisée, les comptes d'administrateur nécessitent toujours une authentification. Cette fonction ne peut pas être désactivée.

Droits de groupe

Le serveur Fiery autorise les actions des utilisateurs en fonction de leur appartenance à un groupe. Chaque groupe est associé à un ensemble spécifique de droits, tels que l'impression en couleur ou en niveaux de gris. Les actions des membres du groupe sont limitées à ces droits. L'administrateur Fiery est habilité à modifier les droits de n'importe quel groupe Fiery, à l'exception des comptes Administrateur et Opérateur.

Dans cette méthode d'authentification utilisateur les différents droits pouvant être attribués à un groupe sont les suivants :

- Imprimer en niveaux de gris : permet aux membres du groupe d'imprimer des tâches en niveaux de gris. Si l'utilisateur ne dispose pas de ce droit, le serveur Fiery 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 : permet aux membres d'un groupe d'imprimer des tâches avec un accès total aux capacités d'impression couleur et niveaux de gouttes variables sur le serveur Fiery. 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 une tâche via FTP (périphériques couleur uniquement).

- Boîte de messagerie Fiery : permet aux membres d'un groupe de disposer de boîtes de messagerie individuelles. Le Fiery Server crée une boîte 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 : permet aux membres d'un groupe de créer des préréglages pour le serveur. Les membres du groupe ont accès à ces préréglages de serveur.
- 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.

Les administrateurs disposant de droits élevés peuvent personnaliser ces fonctionnalités pour restreindre les accès non autorisés et appliquer les protocoles de sécurité de l'organisation.

Utilisateurs locaux

Le logiciel du serveur Fiery interagit avec des types d'utilisateurs uniques, distincts des utilisateurs ou des rôles Windows. Les administrateurs Fiery doivent modifier rapidement tous les mots de passe par défaut après l'installation initiale. L'accès au serveur Fiery par mot de passe doit être strictement appliqué.

- La longueur maximale du mot de passe pour les comptes « Administrateur » et « Opérateur » est de 64 caractères lors de l'utilisation de **Configure** > **Sécurité**.
- La longueur maximale du mot de passe pour les comptes utilisateurs locaux est de 64 caractères lors de l'utilisation de **Configure** > **Comptes utilisateurs**.
- Les mots de passe de l'administrateur et de l'opérateur peuvent être modifiés dans **Configure** > **Comptes utilisateur**.

Comptes d'utilisateurs Fiery locaux et droits d'accès

- Administrateur : Contrôle complet des fonctionnalités du serveur Fiery, avec possibilité de modifier les droits des groupes Fiery, à l'exception des comptes Administrateur et Opérateur.
- Opérateur : mêmes droits que l'administrateur, mais n'a pas accès à la configuration du serveur ni à la suppression du journal des tâches.
- Opérateur de l'imprimante (serveurs Fiery XB uniquement) : gère les tâches de la presse, avec des droits spécifiques ajoutés par l'administrateur.
- Administrateur de service Fiery (serveurs Windows uniquement) : un compte administrateur masqué pour l'installation du certificat de confiance, ne peut pas se connecter au serveur Fiery, apparaît dans les outils de numérisation réseau et peut être supprimé.
- Fiery_SMB_User : compte d'impression Windows par défaut (SMB) qui offre une visibilité sur les files d'attente d'impression du serveur Fiery via le voisinage réseau.
- Invité (par défaut, sans mot de passe) : Dispose des mêmes droits que l'Opérateur, mais ne peut pas accéder aux journaux des tâches, effectuer de modifications, apporter de changements d'état ou prévisualiser les tâches.

Authentification LDAP

Le serveur Fiery utilise LDAP version 3 (conforme à la RFC 2251) pour communiquer avec les serveurs de l'entreprise. Grâce à LDAP v3, il récupère les adresses e-mail des utilisateurs pour les fonctionnalités de numérisation, ainsi que les informations sur les utilisateurs et les groupes pour l'authentification. Cette fonctionnalité est prise en charge exclusivement pour les connexions LDAP vers des serveurs Active Directory.

Le serveur Fiery prend en charge les méthodes d'authentification suivantes via LDAP :

- Automatique
- SIMPLE
- GSSAPI

Le tableau suivant présente les différentes méthodes d'authentification LDAP :

Méthode d'authentification	**Description**	**Serveur Active Directory**
Automatique	Cette option sélectionne GSSAPI ou SIMPLE en fonction de la méthode d'authentification prise en charge par le serveur LDAP.	Pris en charge
SIMPLE	Le mot de passe est requis. Si LDAP est sélectionné via TLS, le mot de passe est chiffré à l'aide de TLS.	Pris en charge
GSSAPI	Cette méthode utilise des tickets Kerberos au lieu de mots de passe, ce qui élimine le besoin de TLS.	Pris en charge

Connexion unique (SSO)

Les serveurs Fiery FS700 Pro prennent en charge le protocole OpenID Connect pour l'authentification utilisateur cloud avec connexion unique (SSO) via Microsoft Entra ID (anciennement Azure AD). Les utilisateurs peuvent se connecter à un Fiery server en utilisant leurs identifiants Entra existants.

Cette méthode d'authentification prend en charge l'authentification multi-facteurs (MFA).

Cette approche de gestion des identités garantit que les serveurs Fiery ne stockent jamais les mots de passe des utilisateurs localement, ce qui renforce considérablement la sécurité.

Mesures de sécurité des données

Pour protéger les informations sensibles, les serveurs Fiery mettent en œuvre les éléments suivants :

Stockage crypté : protège les tâches d'impression et les données de configuration

Le chiffrement des données critiques des clients garantit le stockage sécurisé des mots de passe et des informations de configuration associées sur le serveur Fiery. Ces informations essentielles sont chiffrées ou hachées à l'aide d'algorithmes de chiffrement tels que AES-256 et SHA-2, qui respectent les dernières normes de sécurité.

Les données client stockées sur le disque demeurent inaccessibles, même si le disque est retiré du serveur Fiery. Le cryptage des données utilisateur peut être activé ou désactivé sur les serveurs Fiery sous système d'exploitation Windows. Pour les serveurs Fiery basés sur Linux, la fonctionnalité de chiffrement est toujours activée.

En cas d'oubli d'une phrase secrète utilisée pour la récupération des données, FIERY ne peut pas la réinitialiser, ce qui nécessite une réinstallation complète du logiciel.

Les serveurs fonctionnant sous Windows offrent également une option permettant de chiffrer le lecteur de démarrage contenant le système d'exploitation. Ce chiffrement permet d'éviter les attaques hors ligne sur le serveur Fiery et garantit que le disque de démarrage ne peut pas être utilisé sur un autre périphérique.

Effacement sécurisé : garantit que les données sont irrécupérables après la suppression

En ce qui concerne les serveurs Fiery FS700 fonctionnant sous Linux, 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.

Cette fonctionnalité n'est pas prise en charge sur les serveurs Fiery intégrés utilisant les plateformes matérielles E600 et LX Pro. Ces platesformes stockent les données des documents sur un disque SSD, qui est protégé par un cryptage AES-256. Ce cryptage est toujours activé et ne peut pas être désactivé.

Les serveurs FS700 Pro sous Windows prennent en charge la norme d'assainissement des données NIST 800-88. Les administrateurs Fiery peuvent configurer cette option pour les méthodes de remplacement d'image à 1 ou 3 passages.

Remarque : Les plateformes Fiery XB ou les disques SSD sur lesquels les données utilisateur sont stockées ne prennent pas en charge la fonctionnalité d'effacement sécurisé.

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

Flux de production	Effacement sécurisé
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

Sécurité du réseau

Les serveurs Fiery utilisent les mécanismes de sécurité suivants pour protéger les communications réseau :

- Filtrage IP et gestion des ports
- Configuration du pare-feu
- Prise en charge de SNMP v3 pour des outils de surveillance et de gestion réseau sécurisés

Protocoles réseau pris en charge

Les imprimantes FS700/FS700 Pro prennent en charge un large éventail de protocoles réseau standard afin de garantir la compatibilité, la sécurité et une communication efficace dans divers environnements. Ces méthodes sont les suivantes :

- **Protocoles de base :** TCP/IP, IPv4, IPv6
- **Protocoles Web :** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **Services de fichiers et d'impression :** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Port 9100
- **Gestion et surveillance :** SNMP v1, v2c et v3
- **Accès à distance :** RDP (serveurs basés sur Windows uniquement)
- **Sécurité et authentification :** IPSec (IKEv2), LDAP v3, IEEE 802.1X
- **Services réseau :** DHCP, DNS
- **Protocoles de découverte :** WSD, Bonjour, SLP

Ports réseau

Par défaut, tous les ports TCP/IP inutilisés sont désactivés. L'administrateur Fiery peut activer et désactiver des ports réseau. La désactivation d'un port empêche les connexions externes qui nécessitent l'utilisation de ce port spécifique.

Ports entrants

Les serveurs Fiery supervisent et surveillent les connexions réseau entrantes, en autorisant uniquement le trafic autorisé à accéder au serveur et en le protégeant contre les accès non autorisés ou les attaques.

TCP	UDP	Nom du port	Services associés
20-21		FTP	FTP
80		HTTP	WebTools, IPP

TCP	UDP	Nom du port	Services associés
135		MS RPC	Service Microsoft® RPC. Un port supplémentaire compris entre 49152 et 65535 sera ouvert pour le service Pointer-imprimer associé au protocole SMB.
137-139		NETBIOS	Impression Windows. Ces ports sont fermés par défaut car NetBIOS n'est pas sécurisé.
	161, 162	SNMP	Outils SNMP
	427	SLP	Protocole SLP Il s'agit d'un port bloqué par défaut car SLP n'est pas sécurisé.
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB par TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impression via LPR
631		IPP	IPP
3389		RDP	Bureau à distance (serveurs Fiery basés sur Windows uniquement)
3702	3702	WS-Discovery	Services Web pour périphériques (WSD) Permet la détection et l'impression sur le serveur Fiery via WSD.
	4500	IPsec par NAT traversal	IPsec
	5353	DNS multidiffusion (mDNS)	Bonjour
6310		Port DMP	Impression mobile directe
8010		Ports FIERY	JDF
8021-8022		Ports FIERY	Fiery Harmony, Fiery HotFolders et Fiery Command WorkStation
8090		Ports FIERY	OFA
9100-9103		Port d'impression	Port 9100
	9906	Ports FIERY	Découverte de l'harmonie
21030		Ports FIERY	Fiery Image Viewer

Remarque : Les ports IPSec (500 et 4500) ne sont configurables que pour les modèles FS700 (serveurs Fiery sous Linux).

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 ou désactiver les différents services dépendants fournis par le serveur Fiery.

Ports sortants

Les serveurs Fiery gèrent et limitent le trafic réseau sortant afin que seules les communications autorisées quittent le périphérique, réduisant ainsi l'exposition aux menaces externes.

Ports sortants	Objectif	Configuration par défaut/activée
53	DNS	Valeur par défaut
67	DHCP	Valeur par défaut
80, 443	Mises à jour du système Fiery, JDF, PrintMe et autres communications cloud	Valeur par défaut
161, 162	SNMP	Dans une configuration à double adresse IP
21	Numérisation vers FTP	Configuration activée
123	NTP	Configuration activée
389/636	Services LDAP	Configuration activée
445	Numérisation vers SMB/Journal des tâches vers SMB/JDF Chemin général commun	Configuration activée
500/4500	IPSec	Configuration activée
8080/8443	Port proxy HTTP/HTTPS/FTP	Configuration activée

Communication avec les services cloud

Cette liste répertorie les services et applications Fiery qui nécessitent une communication avec des services cloud externes, par exemple pour télécharger les mises à jour de sécurité Fiery ou pour l'activation des licences. Cette documentation est particulièrement utile pour les clients qui ont désactivé toutes les communications externes et qui tentent d'effectuer des exceptions dans leur pare-feu d'entreprise.

Service/ Application Fiery	Nom de domaine pleinement qualifié	Port	Emplacement du serveur	Informations d'utilisation
Mise à jour système	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Télécharger les mises à jour de sécurité Fiery
OFA	https://flexlicensing.fiery.com	443	Fiery	Activation de la licence
IQ	https://iq.fiery.com/iq	443	AWS	Cloud Fiery IQ

Service/ Application Fiery	Nom de domaine pleinement qualifié	Port	Emplacement du serveur	Informations d'utilisation
LINQ	https://ews.fiery.com	443	Azure	Analyse
Impression universelle	Plusieurs domaines : •portal.azure.com •print.print.microsoft.com •notification.print.microsoft.com •discovery.print.microsoft.com •graph.print.microsoft.com	80/443	Azure	Proxy IPP et service d'impression universelle
SSO	login.microsoft.com	80/443	Microsoft	Connexion unique
Services de mise à jour Windows (Windows Server Update Services, WSUS)	Plusieurs domaines : •http://windowsupdate.microsoft.com •http://.windowsupdate.microsoft.com •https://.windowsupdate.microsoft.com •http://.update.microsoft.com •https://.update.microsoft.com •http://.windowsupdate.com •http://download.windowsupdate.com •https://download.microsoft.com •http://.download.windowsupdate.com •http://wustat.windows.com •http://ntservicepack.microsoft.com •http://go.microsoft.com •http://dl.delivery.mp.microsoft.com •https://dl.delivery.mp.microsoft.com •http://.delivery.mp.microsoft.com •https://.delivery.mp.microsoft.com	80/443	Microsoft	Mises à jour Windows
Command WorkStation	Plusieurs domaines : • https://help.fiery.com •https://learning.fiery.com •https://communities.fiery.com/s/ •https://liveupdate.fiery.com •https://iq.fiery.com	443	Fiery	

Filtrage IP

Le filtrage IP permet à l'administrateur de contrôler les demandes de connexion au serveur Fiery en fonction d'adresses IP prédéfinies. En définissant des stratégies par défaut, l'administrateur peut spécifier si les paquets de données entrants doivent être autorisés ou refusés. De plus, ils peuvent créer des filtres pour un maximum de 16 adresses ou plages IP, en autorisant ou en refusant les demandes de connexion en conséquence.

Chaque paramètre de filtre IP spécifie une adresse IP ou une plage d'adresses IP ainsi que l'action correspondante. Lorsque l'action est refusée, les paquets dont l'adresse source appartient aux adresses spécifiées sont rejetés. Inversement, lorsque l'action est acceptée, les paquets sont autorisés.

Authentification réseau

SNMP v3

Le serveur Fiery prend en charge la dernière norme SNMPv3, ce qui facilite le cryptage des paquets de communication afin de garantir la confidentialité, l'intégrité et l'authentification des messages.

L'administrateur Fiery peut choisir entre trois niveaux de sécurité SNMP : Minimum, Moyen et Maximum. À ces niveaux, les mots de passe sont hachés à l'aide d'algorithmes tels que SHA-1 ou SHA-256, et l'intégralité du message SNMP est cryptée. De plus, l'administrateur local peut configurer les noms de communauté SNMP en lecture et en écriture, ainsi que d'autres paramètres de sécurité.

IEEE 802.1x

La norme 802.1X est une norme IEEE pour le contrôle d'accès réseau basé sur des ports, qui garantit que les périphériques s'authentifient avant d'accéder au réseau local et à ses ressources. Sur les serveurs Fiery, la norme 802.1X peut être configurée pour utiliser EAP-MD5 Challenge ou PEAP-MSCHAPv2 pour l'authentification basée sur le serveur, ou EAP-TLS pour l'authentification basée sur les certificats afin d'améliorer la sécurité. Les serveurs Fiery prennent uniquement en charge le certificat utilisateur (et non le certificat du périphérique) pour l'authentification EAP-TLS basée sur un certificat.

Le serveur Fiery procède à l'authentification au démarrage ou chaque fois que la connexion réseau est déconnectée puis reconnectée.

Chiffrement réseau

Internet Protocol Security (IPsec)

IPsec renforce la sécurité des communications basées sur IP en chiffrant et en authentifiant chaque paquet au niveau réseau, protégeant ainsi les données en transit pour toutes les applications utilisant IP. Le serveur Fiery utilise une authentification par clé pré-partagée pour établir des connexions sécurisées avec d'autres systèmes via IPsec. Une fois la communication IPsec établie entre un ordinateur client et un serveur Fiery, toutes les communications, y compris les tâches d'impression, sont transmises de manière sécurisée sur le réseau.

HTTPS

Les serveurs Fiery sécurisent les communications entre les clients et les composants du serveur à l'aide du protocole HTTPS via TLS. Cela garantit que toutes les données transmises, telles que les tâches d'impression, les mises à jour de statut de la tâche et les commandes administratives, sont cryptées en transit, ce qui les protège contre l'interception ou la falsification. Les serveurs Fiery prennent en charge TLS 1.3 et TLS 1.2, offrant une protection cryptographique solide et des fonctionnalités de sécurité modernes. HTTPS est obligatoire pour les connexions aux WebTools et aux API Fiery, ce qui garantit que le trafic administratif et opérationnel est transmis en toute sécurité.

Gestion de certificats

Les serveurs Fiery offrent une interface pour la gestion des certificats utilisés lors des communications TLS. Les serveurs Fiery prennent en charge les certificats X.509 au format PEM, codés en Base64, à l'aide de clés RSA d'une longueur de 4096, 3072 ou 2048 bits.

La gestion des certificats permet à l'administrateur Fiery d'effectuer les actions suivantes :

- Générer des certificats numériques auto-signés.
- Ajouter un certificat et la clé privée associée pour le serveur Fiery.
- Ajouter, parcourir, afficher et supprimer des certificats d'une autorité de certification approuvée.

Les certificats numériques auto-signés assurent le chiffrement, mais n'offrent pas de validation automatique de la confiance. Pour des déploiements sécurisés, nous vous recommandons d'utiliser des certificats émis par une autorité de certification de confiance afin de garantir une vérification d'identité appropriée.

Une fois qu'un certificat a été signé par une autorité de certification de confiance, il peut être téléchargé sur le serveur Fiery dans la section Configurer des WebTools.

Serveur de messages SMB (Server Message Block)

SMBv1, le protocole hérité pour le partage de fichiers et d'imprimantes, est désactivé sur les serveurs Fiery en raison de failles de sécurité connues. Les serveurs Fiery prennent en charge SMBv2 et SMBv3 à la place. La signature SMB est appliquée, ce qui garantit que tous les paquets sont signés numériquement afin d'éviter les attaques de l'homme du milieu. Lorsque l'authentification SMB est activée, les utilisateurs doivent fournir un nom d'utilisateur et un mot de passe valides pour accéder aux dossiers et au contenu partagés. Il est également possible de limiter l'impression ou le partage de fichiers via SMB pour un compte invité en définissant un mot de passe dans Fiery Configure.

Sécurité matérielle

Les serveurs Fiery sont conçus pour offrir une sécurité matérielle de niveau professionnel. La protection des informations sensibles ne se limite pas aux contrôles logiciels ; les composants matériels jouent un rôle essentiel dans le maintien de l'intégrité du système et de la confidentialité des données. Les principaux éléments matériels et leurs mesures de sécurité sont décrits ci-dessous.

Mémoire volatile (RAM)

Les serveurs Fiery utilisent la mémoire volatile (RAM) pour stocker temporairement les données pendant les opérations actives. Pour atténuer le risque d'exposition des données :

- Les informations sensibles de la mémoire vive sont effacées immédiatement après utilisation ou lors de l'arrêt du système.
- Les techniques d'épuration de la mémoire sont appliquées pour empêcher la persistance des données résiduelles.
- L'accès à la RAM est limité par la séparation des droits imposée par le processeur et le système d'exploitation.

Mémoire non volatile et stockage de données

La mémoire non volatile, y compris les disques durs, les disques SSD et les autres systèmes de stockage persistants, conserve les données même lorsque le système est hors tension. Les mesures de sécurité comprennent :

- Chiffrement des données utilisateur (UDE) pour protéger les données stockées.
- Méthodes de suppression sécurisées pour rendre irrécupérables les informations sensibles lorsque les fichiers sont supprimés.

Mémoire flash

La mémoire flash est utilisée pour stocker le microprogramme, les fichiers de configuration et les paramètres système. Pour maintenir sa sécurité :

- Le micrologiciel est signé numériquement pour éviter toute falsification.
- Les mises à jour du micrologiciel sont vérifiées à l'aide de sommes de contrôle cryptographiques avant l'installation.
- Les mécanismes de protection en écriture empêchent les modifications non autorisées pendant l'exécution.

CMOS et NVRAM

Les paramètres système critiques, tels que les configurations matérielles et les paramètres de démarrage, sont stockés dans le CMOS et la mémoire non volatile (NVRAM). Pour sécuriser ces données :

- L'accès est limité aux processus administratifs autorisés.
- Les mécanismes de démarrage sécurisés garantissent que seules des lectures et des écritures fiables du micrologiciel sont effectuées dans ces zones.
- Les variables NVRAM critiques sont sauvegardées et leur intégrité est vérifiée afin d'éviter toute corruption ou altération malveillante.

Disques de stockage

Les serveurs Fiery utilisent des disques de stockage pour stocker le système d'exploitation et les fichiers système. Ces lecteurs sont également utilisés pour le spoule des tâches, les journaux et les fichiers temporaires.

Les fonctionnalités de sécurité suivantes sont fournies pour protéger les données des clients :

- Chiffrement au niveau du lecteur.
- Des listes de contrôle d'accès (ACL) pour restreindre les opérations de lecture/écriture non autorisées.
- Kits de sécurité de disque dur (en option pour les serveurs Fiery externes) qui améliorent la sécurité du système en permettant aux utilisateurs de verrouiller en toute sécurité les disques du serveur pendant leur fonctionnement normal.

Ports physiques

Les ports physiques, tels que les ports USB, les interfaces réseau et les connecteurs de service, sont des vecteurs potentiels d'accès non autorisé. La sécurité matérielle Fiery permet de remédier à ce risque en :

- Désactivation des ports inutilisés au niveau du matériel ou du micrologiciel.
- Nécessitant une autorisation administrative pour connecter des périphériques externes.
- Surveillance et journalisation de toutes les interactions avec les interfaces physiques critiques.

En intégrant ces mesures de sécurité matérielle aux protections logicielles et réseau, les serveurs Fiery offrent une stratégie complète de défense en profondeur, garantissant la confidentialité, l'intégrité et la disponibilité des données sensibles dans les environnements d'impression.

Intégrité du système et mises à jour sécurisées

Le maintien de l'intégrité du système est primordial pour garantir la sécurité. Les serveurs Fiery offrent les fonctions suivantes :

- Journaux d'audit de sécurité
- Démarrage sécurisé : garantit que seuls les logiciels fiables sont chargés.
- Mises à jour signées numériquement : empêche la falsification des mises à jour logicielles.
- Gestion automatisée des mises à jour de sécurité : simplifie le processus d'application des mises à jour de sécurité.

Journal d'audit de sécurité

Les administrateurs disposant de droits élevés peuvent accéder aux événements de sécurité enregistrés dans le journal d'audit de sécurité et les examiner. Ce journal est activé par défaut.

Chaque événement de sécurité est classé comme Information, Avertissement ou Erreur. L'administrateur ne reçoit aucune alerte ou notification ; au lieu de cela, un journal statique leur est présenté.

Les journaux sont mis en forme pour assurer la compatibilité avec les outils de gestion des informations et des événements de sécurité (SIEM) couramment utilisés pour la collecte et l'analyse des journaux. Toutes les données d'événements capturées sont conformes aux normes définies dans la norme NIST SP 800-53.

L'administrateur Fiery peut accéder au journal d'audit de sécurité sans l'intervention de FIERY. Les journaux pour les serveurs basés sur Linux sont fournis au format Syslog (RFC 5424 ou RFC 3164). Pour les serveurs basés sur Windows, les journaux sont enregistrés au format EVTX standard de Windows et peuvent être consultés via le Gestionnaire des événements Windows ainsi que de nombreuses solutions commerciales exploitant l'API Journal des événements Windows. Les serveurs Fiery sous Linux offrent la possibilité de transmettre les journaux vers un système de collecte centralisé, tel que Syslog.

Les journaux de sécurité sont conservés en fonction de la capacité de stockage local qui leur est attribuée. Lorsque la taille du journal dépasse la limite de stockage prédéfinie (400 Mo), les événements les plus anciens sont automatiquement supprimés.

Démarrage sécurisé

Cette fonctionnalité garantit l'intégrité des fichiers du système d'exploitation lors du démarrage en autorisant uniquement le chargement des composants approuvés et signés numériquement. Sur les serveurs Fiery, il bloque l'exécution de code non autorisé ou malveillant pendant le démarrage, ce qui renforce la sécurité et réduit le risque de compromission. Par défaut, le démarrage sécurisé est désactivé.

Mises à jour signées numériquement

Les serveurs Fiery utilisent des mises à jour signées numériquement pour garantir l'intégrité et l'authenticité de toutes les installations de logiciels et de micrologiciels. Chaque mise à jour est signée de manière cryptographique par Fiery ou ses partenaires agréés, ce qui permet au serveur de vérifier que le contenu n'a pas été modifié ou altéré. Ce processus protège contre l'introduction de code malveillant et garantit que seules des mises à jour fiables sont appliquées, ce qui maintient la sécurité et la fiabilité du système.

Gestion automatisée des mises à jour de sécurité

La mise à jour en temps voulu des logiciels est essentielle au fonctionnement optimal des serveurs Fiery. L'installation de toutes les mises à jour de sécurité est essentielle pour garantir la sécurité des serveurs Fiery dans tout environnement d'impression.

Mises à jour du système Fiery télécharge et installe les mises à jour de sécurité si l'option est activée sur le serveur Fiery. Cette option est activée par défaut et nous recommandons à nos clients de la laisser activée.

Les vulnérabilités de sécurité du système d'exploitation Microsoft® Windows™ ne sont pas détaillées dans ce document, car elles sont gérées directement par Microsoft et distribuées aux clients via les **mises à jour Windows** dès qu'elles sont disponibles.

Pour répondre aux préoccupations et aux vulnérabilités de sécurité susceptibles d'affecter les composants matériels essentiels des systèmes Fiery, notamment la carte mère, le processeur et le microprogramme, Fiery collabore étroitement avec les fabricants afin d'obtenir les mises à jour de sécurité requises. Ces mises à jour de sécurité sont ensuite fournies aux clients si nécessaire.

Remarque : Les mises à jour logicielles Fiery sont signées numériquement à l'aide de l'algorithme de hachage sécurisé (SHA-2) afin d'éviter toute modification non autorisée, y compris l'insertion de logiciels malveillants.

Mises à jour de sécurité du logiciel serveur Fiery

Des mises à jour logicielles régulières sont essentielles au bon fonctionnement du serveur Fiery. L'application des dernières mises à jour de sécurité logicielles du serveur Fiery garantit l'intégrité du système, les vulnérabilités sont atténuées et la conformité aux normes de sécurité du secteur est maintenue.

L'équipe de sécurité du serveur Fiery surveille et suit avec diligence les vulnérabilités de sécurité grâce à un réseau complet de sources fiables et fiables, telles que :

- Alertes et avis de l'Agence américaine sur la cybersécurité et la sécurité des infrastructures (CISA)
- Base de données sur la vulnérabilité nationale de l'Institut national des normes et de la technologie (NIST) des États-Unis
- Enregistrements des vulnérabilités et expositions communes (CVE)
- Rapports et avis du Centre de coordination (CERT/CC) sur les vulnérabilités logicielles et matérielles
- Gouvernement régional et organismes de réglementation
- Avis de sécurité des fournisseurs de logiciels et de matériel

Fiery hiérarchise les correctifs de sécurité en fonction de la sévérité (critique, élevée, moyenne et faible), telle que déterminée par le système de notation de vulnérabilité commun (CVSS). Ces correctifs sont publiés après avoir obtenu l'approbation correspondante du partenaire du fabricant d'équipements d'origine (OEM). Une fois approuvées, les mises à jour de sécurité du logiciel Fiery sont mises à disposition pour téléchargement. Toutes les mises à jour logicielles Fiery sont signées numériquement à l'aide de l'algorithme de hachage sécurisé SHA-2 afin d'empêcher toute modification non autorisée, y compris l'insertion de logiciels malveillants.

Lorsque cette fonction est activée, Mises à jour du système Fiery télécharge et installe automatiquement les mises à jour de sécurité sur le serveur Fiery. Cette option est activée par défaut et nous recommandons vivement aux clients de conserver son statut actif.

Conformité et meilleures pratiques

Les implémentations de sécurité robustes sont conformes aux normes standards de l'industrie et aux cadres réglementaires, notamment :

- RGPD, loi sur les données de l'UE
- ISO/IEC 27001 (FS700 Pro uniquement)
- FIPS 140-2
- NIST 800-88. Directives pour l'assainissement des supports (FS700 Pro uniquement)
- NIST 800-52. Directives pour la sélection, la configuration et l'utilisation des implémentations TLS (Transport Layer Security)
- NIST 800-171. Protection des informations non classifiées contrôlées dans les systèmes et organisations non fédéraux (FS700 Pro uniquement)
- Certification du modèle de maturité en matière de cybersécurité (CMMC) du département de la Défense des États-Unis. Niveau 2 : Protection étendue des informations non classifiées contrôlées (CUI) (FS700 Pro uniquement)
- NIST 800-193. Directives de résilience du micrologiciel de la plateforme (FS700 Pro uniquement)
- NIST 800-53. Contrôles de sécurité et de confidentialité pour les systèmes d'information et les organisations
- Profil de protection Critères communs pour les systèmes d'exploitation à usage général (FS700 Pro uniquement)

Pour renforcer la posture de sécurité, les administrateurs informatiques sont responsables de la mise en œuvre des mesures suivantes :

- Application régulière des mises à jour de sécurité
- Application de stratégies d'authentification robustes
- Réalisation d'audits de sécurité périodiques
- Mise en œuvre de la segmentation du réseau pour les environnements d'impression

Directives pour une configuration sécurisée du serveur Fiery

Les administrateurs Fiery peuvent suivre ces instructions pour renforcer la sécurité lors de la configuration du serveur Fiery :

Changer le mot de passe administrateur

Les serveurs Fiery sont livrés depuis l'usine avec un mot de passe par défaut pour le compte administrateur. Ce mot de passe confère un accès complet au serveur Fiery, à la fois localement et depuis un client distant. Cet accès comprend, sans s'y limiter :

- Système de fichiers (serveurs Fiery sous Windows uniquement)
- Paramètres de sécurité du système
- Paramètres de l'application
- Entrées de registre

Nous recommandons vivement de modifier le mot de passe par défaut de l'administrateur Fiery immédiatement après l'installation, puis à intervalles réguliers, conformément aux politiques de sécurité de votre organisation. Le mot de passe de l'administrateur Fiery doit être modifié dans la plateforme Fiery.

Meilleures pratiques en matière d'exploitation sécurisée et efficace

- Limitez SNMP à la version 3 pour une sécurité maximale.
- Désactivez WSD pour la soumission des tâches afin d'éviter son utilisation dans les flux de production d'impression.
- Désactivez les protocoles d'impression Windows (LPR, port 9100, IPP), sauf si cela est explicitement requis.
- Activez le filtrage du port TCP/IP pour bloquer les ports inutilisés et réduire les risques.
- Fermez les ports 137-139 et 445 si vous n'en avez pas besoin pour l'impression Windows ou le partage de fichiers.
- Désactivez HTTP sur le port 80 afin d'empêcher les communications non sécurisées.
- Activez l'impression sécurisée afin que seul le propriétaire de la tâche puisse libérer les tâches d'impression.

Environnements de haute sécurité

Les administrateurs disposant de droits élevés peuvent facilement configurer des paramètres de haute sécurité en sélectionnant le profil de haute sécurité disponible dans **WebTools** > **Configurer** > **Sécurité**.

Conclusion

Bien que dotés de fonctionnalités de sécurité avancées, les serveurs Fiery ne sont pas conçus pour être exposés directement à Internet. Ils doivent être déployés dans un environnement réseau sécurisé, avec un accès strictement contrôlé par l'administrateur réseau. Conçus pour répondre aux dernières normes du secteur, les serveurs Fiery offrent une sécurité de niveau entreprise pour protéger les environnements d'impression contre les cybermenaces en constante évolution. Les administrateurs peuvent garantir la conformité et protéger les données sensibles en tirant pleinement parti des capacités de sécurité de Fiery.

Nouveautés de FS700, FS700 Pro

- Les modules principaux du système ont été mis à jour pour corriger les failles de sécurité.
- La fonctionnalité de messagerie a été abandonnée afin d'éviter les attaques par e-mail et de garantir la conformité aux réglementations de sécurité.
- Toutes les communications avec le serveur Fiery peuvent désormais être cryptées à l'aide de TLS 1.3. Les connexions du Bureau à distance aux serveurs Fiery fonctionnant sous Windows 10 prennent actuellement en charge TLS 1.2.
- Ajout de la prise en charge de TLS 1.3 aux applications et modules Fiery suivants :
  - Components du serveur de licences et du client
  - Proxy IPP : requis pour l'impression universelle Microsoft
  - Protocole d'authentification réseau 802.1x
  - EFI LINQ : utilisé pour créer des rapports de plantage sur le serveur Fiery
  - JDF
  - Mise à jour système
  - FCC – Fiery Cloud Connector
- Les outils IPsec utilisés sur les serveurs Linux ont été remplacés par des outils plus récents et plus sécurisés.
- Ajout de la prise en charge de l'AES (Norme avancée de chiffrement) pour les communications SNMPv3 et nouvelle valeur par défaut d'AES 128 :
  - AES 128 (par défaut)
  - AES 192 (l'utilisateur peut choisir dans Configure)
  - AES 256 (l'utilisateur peut choisir dans Configure)
  - DES est toujours pris en charge, bien qu'il ne soit plus l'option par défaut. Les utilisateurs peuvent le sélectionner si nécessaire.