Documento técnico sobre seguridad de Fiery

Servidores Fiery FS200 Pro /FS200

Fecha de publicación: Mayo de 2018

Serie de documentos técnicos

Documento técnico sobre seguridad de Fiery

Contenido

1 Descripción general del documento

Este documento ofrece a los usuarios finales una descripción general de la arquitectura y aspectos funcionales del servidor Fiery® en relación a la seguridad del dispositivo en los servidores Fiery FS200/FS200 Pro. Trata temas como el hardware, seguridad de red, control de acceso y seguridad del sistema operativo y los datos.

El objetivo del documento es ayudar a los usuarios finales a comprender todas las funciones de seguridad del servidor Fiery de las que pueden beneficiarse y a conocer sus posibles vulnerabilidades.

1.1 Filosofía de seguridad de EFI

EFI™ sabe que hoy en día, la seguridad es una de las principales preocupaciones de las empresas de todo el mundo, y por ello hemos incorporado potentes funciones de seguridad en los servidores Fiery para proteger los activos más valiosos de las empresas. Además trabajamos de forma proactiva con nuestros socios de OEM internacionales y nuestros equipos multidisciplinares para determinar las necesidades actuales y futuras de las empresas en materia de seguridad, a fin de que ésta no se convierta en un problema para nuestros productos.
Como siempre, seguimos recomendando que los usuarios finales combinen las funciones de seguridad de Fiery con otras protecciones, como la contraseña de seguridad y potentes procedimientos de seguridad física, con el fin de lograr una seguridad óptima para todo el sistema.

1.2 Configuración de la función de seguridad mediante Fiery Configure

Los usuarios de Fiery que tienen acceso al servidor Fiery a través de Fiery Command WorkStation® con un inicio de sesión de administrador pueden configurar todas las funciones de Fiery a través de Fiery Configure. Fiery Configure puede iniciarse desde Fiery Command WorkStation o WebTools™ dentro de la pestaña Configure.

2 Seguridad física y del hardware

2.1 Memoria volátil

El servidor Fiery utiliza memoria RAM volátil para la memoria local de la CPU y para el sistema operativo, el software del sistema del Fiery y la memoria de trabajo de los datos de imagen. Los datos que se escriben en la RAM se conservan mientras la alimentación esté conectada. Cuando se desconecta la alimentación, se eliminan todos los datos.

2.2 Memoria no volátil y almacenamiento de datos

El servidor Fiery contiene varios tipos de tecnologías de almacenamiento de datos no volátil para conservar los datos en el servidor Fiery cuando se desconecta la alimentación. Estos datos incluyen la información de programación del sistema y los datos de usuario.

2.2.1 Memoria flash

La memoria flash almacena el programa de autodiagnóstico y arranque (BIOS) y algunos datos de configuración del sistema. Este dispositivo se programa en fábrica y sólo puede reprogramarse mediante la instalación de módulos de actualización especiales creados por EFI. Si los datos se dañan o se eliminan, el sistema no se inicia.

Una parte de la memoria flash también se utiliza para registrar el
uso de la llave de protección de software para activar las opciones de software de Fiery.

Ningún dato del usuario se almacena en este dispositivo y el usuario
no tiene acceso de datos al mismo.

2.2.2 CMOS

La memoria CMOS con batería se utiliza para almacenar la configuración de máquina del servidor. Ninguna de esta información se considera confidencial ni privada. Los usuarios pueden acceder a estos valores en un servidor Windows 8.1 Pro a través de Fiery Integrated Workstation (el kit FACI que incluye monitor, teclado y ratón) si está instalada.

2.2.3 NVRAM

Hay varios pequeños dispositivos NVRAM en el servidor Fiery que contienen firmware operativo. Estos dispositivos contienen información operativa específica que no es relativa al cliente. El usuario no tiene acceso a los datos contenidos en los mismos.

2.2.4 Unidad de disco duro

Durante las operaciones normales de impresión y escaneado así como durante la creación de información de administración de trabajos, los datos de imagen se escriben a un área aleatoria de la unidad de disco duro.

Los datos de imagen y la información de administración de trabajos puede ser eliminada por un operador o al final de un periodo de tiempo predefinido, haciendo que los datos de imagen ya no sean accesibles.

Para proteger los datos de imagen del acceso no autorizado, EFI ofrece la función Borrado seguro (consulte la sección 6.2.4). Una vez habilitada por el administrador del sistema, la operación seleccionada se lleva a cabo en el momento adecuado para eliminar de forma segura los datos borrados del disco duro.

2.2.5 Puertos físicos

El servidor Fiery puede conectarse mediante los siguientes puertos externos:

Puertos Fiery	Función	Acceso	Control de acceso
Conector Ethernet RJ-45	Conectividad Ethernet	Conexiones de red (consulte las conexiones de impresión y red más adelante)	Utilice el filtrado IP de Fiery para controlar el acceso
Conector de interfaz de la copiadora	Imprimir/ Escanear	Dedicado al envío/ recepción a/de el mecanismo de impresión	N/D
Puerto USB	Conexión del dispositivo USB	Conector Plug-and-play diseñado para su uso con dispositivos multimedia extraíbles opcionales	La impresión USB puede desactivarse. El acceso a los dispositivos de almacenamiento USB pueden desactivarse mediante la directiva de grupo de Windows.

2.3 Interfaz local

El usuario puede acceder a las funciones de Fiery a través del kit FACI (si está habilitado en un servidor Windows 8.1 Pro) o mediante el LCD Fiery de los servidores Fiery. El acceso a la seguridad del servidor Fiery con el kit FACI se controla mediante la contraseña de administrador de Windows, si el kit FACI está habilitado. El LCD Fiery ofrece funciones muy limitadas que no suponen ningún riesgo para la seguridad. colaboración con el OEM. El kit opcional permite extraer la unidad de disco duro interna del chasis integrado y montarla en un alojamiento con alimentación externo independiente.

2.4 Opción de kit de disco duro extraíble

El servidor Fiery admite un kit de opción de unidad de disco duro extraíble para aumentar la seguridad. Este kit permite al usuario bloquear las unidades del servidor en el sistema para un funcionamiento normal, así como de retirar las unidades y depositarlas en una ubicación segura tras apagar el servidor.

2.4.1 Para servidores externos

Los servidores Fiery admiten un kit de opción de unidad de disco duro extraíble. La disponibilidad de este kit opcional para un producto Fiery concreto depende de los términos de los contratos de desarrollo y distribución de EFI con cada socio de OEM individual.

2.4.2 Para servidores integrados

Los productos integrados sólo pueden ofrecer la unidad de disco duro extraíble como una opción coordinada con el OEM, ya que la ubicación de montaje y los soportes para la impresora multifuncional (MFP) se deben desarrollar en colaboración con el OEM. El kit opcional permite extraer la unidad de disco duro interna del chasis integrado y montarla en un alojamiento con alimentación externo independiente.

3 Seguridad de red

Las funciones estándar de seguridad de la red incorporadas en el servidor Fiery incluyen la capacidad de permitir el acceso e imprimir en el dispositivo de salida únicamente a los usuarios y grupos autorizados, limitando las comunicaciones de los dispositivos a las direcciones IP especificadas y controlando la disponibilidad de cada uno de los puertos y protocolos de red como se desee.

Aunque los servidores Fiery cuentan con diferentes funciones de seguridad, no es un servidor para su conexión a Internet. Debe instalarse en un entorno protegido y al administrador de la red debe configurar adecuadamente su accesibilidad.

3.1 Puertos de red

El servidor Fiery permite al administrador de red habilitar y deshabilitar de forma selecciona los siguientes puertos IP. Por tanto, es posible bloquear de forma efectiva la comunicación de dispositivos y el acceso al sistema no deseados a través de protocolos de transporte específicos.

TCP	UDP	Nombre de puerto	Servicios dependientes
20–21		FTP	
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service (sólo Windows 8.1 Pro). Se abrirá un puerto adicional en el rango 49152-65536 para ofrecer servicio de Apuntar e imprimir relacionado con SMB.
137–139		NETBIOS	Impresión en Windows
	161, 162	SNMP	WebTools, Fiery Central, algunas utilidades anteriores y otras herramientas basadas en SNMP
	427	SLP	
443		HTTPS	WebTools, IPP/s
445		SMB/IP	SMB a través de TCP/IP
	500	ISAKMP	IPSec
515		LPD	Impresión LPR, algunas utilidades anteriores (como WebTools, versiones anteriores de CWS)
631		IPP	IPP
3050			Firebird
	4500	IPsec NAT	IPSec
	5353	DNS multidestino	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	Puertos EFI	Command WorkStation 4 y 5, Fiery Central, herramientas basadas en EFI SDK, funciones bidireccionales del controlador de impresora Fiery, WebTools, Fiery Direct Mobile Printing y conversión de documentos nativos.
9100–9103		Puerto de impresión	Puerto 9100

Los otros puertos TCP, excepto los especificados por el OEM, están deshabilitados. No se puede acceder de forma remota a ningún servicio que dependa de un puerto deshabilitado.

El administrador de Fiery también puede habilitar y deshabilitar los diferentes servicios de red suministrados por el servidor Fiery.

El administrador local puede definir los nombres de comunidad de lectura y escritura SNMP y otras configuraciones de seguridad.

3.2 Filtrado IP

El administrador puede restringir las conexiones autorizadas con el servidor Fiery desde los hosts cuyas direcciones IP estén dentro de un determinado rango de IP. El servidor Fiery ignora los comandos o trabajos enviados desde direcciones IP no autorizadas.

3.3 Encriptación de red

3.3.1 IPsec

La seguridad IPsec o IP proporciona seguridad para todas las aplicaciones con protocolos IP mediante la encriptación y autentificación de todos y cada uno de los paquetes.

El servidor Fiery utiliza una autentificación de clave precompartida para establecer conexiones seguras con otros sistemas a través de IPsec.

Una vez que se ha establecido la comunicación segura a través de IPsec entre un ordenador cliente y un servidor Fiery, todas las comunicaciones (incluidos los trabajos de impresión) se transmiten de forma segura a través de la red.

* Estos puertos se activan después de haber instalado Fiery Command WorkStation versión 6.2 o posteriores en un servidor Fiery externo.

3.3.2 SSL y TLS

SSL/TLS son protocolos a nivel de aplicación que se utilizan para transmitir de forma segura mensajes a través de Internet. Los servidores Fiery admiten los protocolos SSL v3 y TLS v1.0/v1.1/v1.2.

Algunos servidores Fiery admiten SSL/TLS. Los usuarios pueden acceder de forma segura a la página de inicio del servidor Fiery y las Web API a través de SSL/TLS. Es posible configurar la conexión a servidores LDAP y servidores de correo electrónico para que funcionen a través de SSL/TLS para garantizar una comunicación segura.

3.3.3 Gestión de certificados

Los servidores Fiery ofrecen una interfaz de gestión de certificados para gestionar los certificados utilizados en distintas comunicaciones SSL/TLS. Admite el formato de certificado X.509.

La gestión de certificados permite al administrador de Fiery realizar lo siguiente:

- Certificados digitales autofirmados.
- Añadir un certificado y su clave privada correspondiente para el servidor Fiery.
- Añadir, examinar, ver y eliminar certificados de un centro de certificados de confianza.

3.4 IEEE 802.1x

802.1x es un protocolo estándar IEEE para control del acceso a la red basado en puertos. Este protocolo proporciona un mecanismo de autentificación antes de que el dispositivo consiga acceder a la LAN y sus recursos.

Cuando está habilitado, el servidor Fiery puede configurarse para utilizar EAP MD5-Challenge o PEAP-MSCHAPv2 para solicitar autentificación a un servidor de autentificación 802.1x.

El servidor Fiery realiza la autentificación en el momento del arranque o cuando se desconecta y se vuelve a conectar el cable Ethernet.

3.5 SNMP v3

El servidor Fiery admite SNMPv3, que es un protocolo de red seguro para administrar dispositivos en redes IP. Los paquetes de comunicación SNMPv3 pueden encriptarse para garantizar la confidencialidad. Además garantiza la integridad de los mensajes
y la autentificación.

El administrador de Fiery puede elegir entre tres niveles de seguridad en SNMPv3. El administrador de Fiery también tiene la opción de solicitar autentificación antes de permitir transacciones SNMP y encriptar los nombres de usuario y las contraseñas SNMP.

3.6 Seguridad de correo electrónico

El servidor Fiery admite los protocolos POP y SMTP. Para proteger el servicio frente a ataques o un uso inadecuado, el administrador de Fiery puede habilitar otras funciones de seguridad adicionales como las que se indican a continuación:

3.6.1 POP antes de SMTP

Algunos servidores de correo electrónico sigue admitiendo el protocolo SMTP no seguro, que permite que cualquier persona pueda enviar un mensaje de correo electrónico sin autentificación. Para evitar el acceso no autorizado, algunos servidores de correo electrónico requieren que los clientes de correo electrónico se autentifiquen a través de POP antes de utilizar SMTP para enviar un correo electrónico. Para estos servidores de correo electrónico, el administrador de Fiery tendría que habilitar la autentificación POP antes de SMTP.

3.6.2 OP25B

Outbound Port 25 Blocking (OP25B) es una medida antispam de ISP mediante la cual el ISP puede bloquear paquetes que van al puerto 25 a través de sus routers. La interfaz de configuración de correo electrónico permite al administrador de Fiery especificar un puerto diferente.

4 Control de acceso

4.1 Autentificación de usuario

La función de autentificación de usuario del servidor Fiery permite al servidor Fiery hacer los siguiente:

- Autentificar nombres de usuario.
- Autorizar acciones en función de los privilegios del usuario.

El servidor Fiery puede autentificar usuarios:

- Basados en el dominio: usuarios definidos en un servidor corporativo y los que se accede mediante LDAP.
- Basados en Fiery: usuarios definidos en el servidor Fiery.

El servidor Fiery autoriza las acciones en función del grupo al cual pertenece el usuario. Cada grupo esta asociado con un conjunto de privilegios (por ejemplo, Imprimir en blanco y negro, Imprimir en color o en blanco y negro) y las acciones de los miembros del grupo están limitadas a estos privilegios.

Los grupos de Fiery son grupos de usuarios con un conjunto predefinido de privilegios. El grupo de Fiery asigna una serie de privilegios a un grupo de usuarios.

El administrador Fiery puede modificar los privilegios de cualquier grupo de Fiery, con la excepción de los usuarios Administrador, Operador e Invitado.

Para esta versión de Autentificación de usuario, pueden editarse o seleccionarse los diferentes niveles de privilegios de un grupo como se indica a continuación:

- Imprimir en B/N: Este privilegio permite a los miembros del grupo imprimir trabajos en el servidor Fiery. Si el usuario no tiene el privilegio "Imprimir en color y en B/N", el servidor Fiery fuerza que el trabajo se imprima en blanco y negro (B/N).
- Imprimir en color y en B/N: Este privilegio permite a los miembros del grupo imprimir trabajos en el servidor Fiery con acceso completo a las funciones de impresión en color y en escala de grises de los servidores Fiery. Si no se dispone de ninguno de los dos privilegios anteriores, el trabajo de impresión no se imprime y los usuarios no pueden enviar el trabajo por FTP (sólo dispositivos de color).
- Buzón de Fiery: Este privilegio permite a los miembros del grupo tener buzones individuales. El servidor Fiery crea un buzón en función del nombre de usuario con un privilegio de buzón. Sólo pueden acceder a este buzón los usuarios con el nombre de usuario y la contraseña del buzón.
- Calibración: Este privilegios permite a los miembros del grupo realizar la color.
- Crear valores predefinidos: Este privilegio permite a los miembros del grupo crear Valores predefinidos de servidor para permitir a otros usuarios de Fiery tener acceso a los valores predefinidos de trabajo más utilizados.
- Administrar flujos de trabajo: Este privilegio permite a los miembros del grupo crear, publicar o editar Impresoras virtuales.

Nota: La autentificación de usuario sustituye las funciones de impresión de miembros y grupos.

4.2 Autentificación de Fiery Software

El servidor Fiery define los usuarios Administrador, Operador e Invitado con privilegios diferentes. Estos usuarios son específicos del software Fiery y no están relacionados con usuarios ni funciones definidos en Windows. Se recomienda que los administradores pidan contraseñas para acceder al servidor Fiery. Además, EFI recomienda que el administrador cambie la contraseña por omisión a una contraseña diferente tal como se defina en los requisitos de seguridad del usuario final.

Los tres niveles de contraseñas en el servidor Fiery permiten el acceso a los siguientes privilegios:

- Administrador: Tiene control total sobre rodas las funcionalidades del servidor Fiery.
- Operador: Tiene los mismos privilegios que el administrador, pero no tiene acceso a algunas funciones del servidor, como la configuración, y no puede eliminar el registro de trabajos.
- Invitado (por omisión; sin contraseña): Tiene los mismos privilegios que el operador, pero no puede acceder al registro de trabajos, no puede realizar ediciones ni puede cambiar el estado de los trabajos de impresión ni ver presentaciones preliminares de trabajos.

5 Entorno de sistema operativo

5.1 Procedimientos de puesta en marcha

El sistema operativo y el software del sistema Fiery se cargan desde el disco duro local durante la puesta en marcha.

El BIOS residente en la placa base del Fiery es de sólo lectura y almacena la información necesaria para arrancar el sistema operativo. Cualquier cambio en la BIOS (o la eliminación de la BIOS) impide que el servidor Fiery funcione correctamente.

En la página configuración se indican los valores especificados durante la configuración. Alguna información, como la información de proxy FTP, la información de contraseña y los nombres de comunidad SNMP no se incluyen en la página configuración.

5.2 Linux

Los sistemas Linux no incluyen una interfaz local que permita el acceso al sistema operativo.

5.2.1 Software antivirus para Linux

El sistema operativo Linux utilizado en los servidores Fiery es un sistema operativo dedicado sólo para servidores Fiery. Tiene todos los componentes de sistema operativo que requiere un servidor Fiery, pero no algunos de los componentes de uso general para sistemas Linux, como Ubuntu. Además de ofrecer un mejor rendimiento, este sistema operativo dedicado no presenta la misma vulnerabilidad ante virus que un sistema Linux general o que un sistema operativo Microsoft. Es posible que el software antivirus diseñado para un sistema operativo Linux general no se pueda ejecutar en servidores Fiery.

5.3 Windows 8.1 Pro

El servidor Fiery se suministra con una contraseña de administrador de Windows 8.1 por omisión. Se recomienda que el administrador cambie la contraseña tras la instalación. También es muy recomendable que cambie la contraseña con regularidad para cumplir con la política de TI de la organización. La contraseña de administrador da un acceso total al servidor Fiery localmente y/o una estación de trabajo remota.
Esto incluye, entre otros, el acceso al sistema de archivos, la política de seguridad del sistema y las entradas del registro. Además, este usuario puede cambiar la contraseña de administrador denegando el acceso a otras personas al servidor Fiery.

5.3.1 Actualizaciones de seguridad Microsoft

Microsoft publica periódicamente actualizaciones de seguridad para dar respuesta a las potenciales lagunas de seguridad del sistema operativo Windows 8.1. De forma predeterminada, las actualizaciones de Windows notifican al usuario la disponibilidad de actualizaciones de seguridad, pero no las descargan. El administrador de Fiery puede cambiar esta opción predeterminada en Windows Update o bien instalar manualmente las actualizaciones de seguridad.

5.3.2 Herramientas de SMS

EFI cuenta con su propia herramienta de actualización del sistema dedicada para los sistemas basados en Windows. Esta herramienta gestiona la recuperación de todas las actualizaciones de seguridad de Microsoft y las actualizaciones de software de Fiery aplicables. El servidor Fiery no admite herramientas de SMS de terceros para recuperar y enviar actualizaciones en el servidor Fiery.

5.3.3 Software antivirus para Windows

En general, el software antivirus puede utilizarse con un servidor Fiery. El software antivirus se suministra de muchas formas diferentes y pueden contener muchos componentes y funciones para solucionar un riesgo concreto. Aquí aparecen unas cuantas indicaciones generales para ayudar a los clientes a confiar en el software antivirus que elijan. Recuerde que el software antivirus resulta más útil en una configuración del kit de FACI, donde los usuarios pueden infectar el servidor Fiery con un virus durante las acciones estándar de Windows. Para los servidores Fiery que no tienen un kit FACI, es posible ejecutar un software antivirus en un PC remoto y explorar una unidad de disco duro de servidor Fiery compartida. Sin embargo, EFI sugiere que el administrador de Fiery trabaje directamente con el fabricante del software antivirus para obtener asistencia operativa. A continuación se indican las indicaciones generales de EFI para los diferentes componentes de software antivirus de Windows:

Motor antivirus: Cuando un motor antivirus explora el servidor Fiery, independientemente de si es una exploración programada o no, puede afectar al rendimiento de Fiery.

Antispyware: Un programa antispyware puede afectar al rendimiento de Fiery cuando los archivos llegan a un servidor Fiery. Por ejemplo: trabajos de impresión entrantes, archivos que se descargan durante la actualización del sistema de Fiery o una actualización automática de aplicaciones que se ejecuta en un servidor Fiery.

Firewall integrado: Dado que el servidor Fiery cuenta con un firewall, generalmente no son necesarios firewalls antivirus. EFI recomienda que los clientes trabajen con su propio departamento de TI y consulten la sección 3.1 de este documento si necesitan instalar y ejecutar un firewall integrado que forme parte del software antivirus.

Antispam: Fiery admite funciones de impresión y escaneado a través de correo electrónico. Recomendamos que se utilice un mecanismo de filtrado de correo spam basado en servidor. Los servidores Fiery también pueden configurarse para imprimir documentos desde direcciones de correo electrónico especificadas. No se requiere el componente antispam porque ejecutar un cliente de correo electrónico separado (como por ejemplo Outlook) en el servidor Fiery no es una operación admitida.

Lista blanca y lista negra: Las funcionalidades de lista blanca y lista negra normalmente no tienen efectos adversos en el servidor Fiery. EFI recomienda encarecidamente que el cliente configure esta funcionalidad de forma que no se incluyan módulos Fiery en la lista negra.

HID y control de aplicaciones: Debido a la naturaleza compleja de HID y el control de aplicaciones, la configuración antivirus debe probarse y confirmarse cuidadosamente cuando se utilice cualquiera de estas funciones. Cuando están ajustadas correctamente, HID y el control de aplicaciones son excelentes medidas de seguridad y pueden coexistir con el servidor Fiery. Sin embargo, es fácil provocar problemas en el servidor si se utilizan valores incorrectos de parámetros de HID y exclusiones de archivos incorrectas, causadas muchas veces por "aceptar los valores predeterminados". La solución es revisar las opciones seleccionadas en los valores de HID y el control de aplicaciones junto con la configuración del servidor Fiery, como puertos de red, protocolos de red, ejecutables de aplicaciones, archivos de configuración, archivos temporales, etcétera.

5.4 Virus de correo electrónico

Normalmente, los virus que se transmiten a través de correo electrónico requieren algún tipo de ejecución por parte del receptor. El servidor Fiery descarta los archivos adjuntos que no son archivos PDL. El servidor Fiery también ignora el correo electrónico en formato RTF o HTML o cualquier JavaScript incluido. Aparte de la respuesta de correo electrónico a un usuario específico basada en un comando recibido, todos los archivos recibidos por correo electrónico se tratan como trabajos PDL. Consulte los detalles sobre el flujo de trabajo de impresión de correo electrónico de Fiery en la sección 6.4 de este documento.

6 Seguridad de datos

6.1 Encriptación de información crítica

La encriptación de información crítica en el servidor Fiery garantiza que todas las contraseñas y la información de configuración relacionada sean seguras cuando se almacenan en el servidor Fiery. Se utilizan algoritmos criptográficos compatibles con NIST 2010.

6.2 Impresión estándar

Los trabajos enviados al servidor Fiery se envían a una de las colas de impresión siguientes publicadas por el servidor Fiery:

- Cola En espera
- Cola Impresión
- Cola Impresión secuencial
- Cola directa (conexión directa)
- Impresoras virtuales (colas personalizadas definidas por el administrador de Fiery).

El administrador de Fiery puede deshabilitar las colas Impresión y Directa para limitar la impresión automática. Con las contraseñas habilitadas en el servidor Fiery, esta función limita la impresión a los operadores y administradores de Fiery.

6.2.1 Colas En espera, Impresión e Impresión secuencial

Cuando un trabajo se envía a la cola Impresión o En espera, el trabajo se pone en cola en la unidad de disco duro del servidor Fiery. Los trabajos enviados a la cola En espera se retienen en la unidad de disco duro de Fiery hasta que el usuario envía el trabajo para su impresión o lo elimina mediante una utilidad de administración de trabajos, como Fiery Command WorkStation, Fiery Command WorkStation ME o Clear Server.

La cola Impresión secuencial permite al Fiery mantener el orden de los trabajos en trabajos concretos enviados desde la red. El flujo de trabajo será de tipo FIFO (primero en entrar, primero en salir), en cuanto al orden en el que los trabajos se reciben a través de la red. Cuando no está habilitada la cola Impresión secuencial, los trabajos de impresión enviados a través del Fiery puede perder el orden debido a muchos factores, como por ejemplo, que el Fiery permite que se adelanten trabajos más pequeños mientras trabajos más grandes se quedan en la cola.

6.2.2 Cola Impresos

Los trabajos enviados a la cola Impresión se almacenan en la cola Impresos del servidor Fiery, si está habilitada. El administrador puede definir cuántos trabajos se conservan en la cola Impresos. Cuando la cola Impresos está deshabilitada, los trabajos se eliminan automáticamente tras imprimirse.

6.2.3 Cola directa (conexión directa)

La cola Directa está diseñada para la descarga de fuentes y aplicaciones que requieren la conexión directa al módulo PostScript en los controladores Fiery.

EFI no recomienda imprimir a la cola Directa. Fiery elimina todos los trabajos enviados a través de la conexión directa tras la impresión. Sin embargo, EFI no garantiza que se eliminen todos los archivos temporales relacionados con el trabajo.

Los trabajos de tipos de archivo VDP, PDF o TIFF se redirigen a la cola Impresión cuando se envían a la cola Directa. Los trabajos enviados a través del servicio de red SMB pueden redirigirse a la cola Impresión cuando se envían a la cola Directa.

6.2.4 Eliminación de trabajos

Cuando se borra un trabajo de Fiery de forma automática o mediante las herramientas de Fiery, el trabajo no se puede visualizar ni recuperar mediante las herramientas de Fiery. Si el trabajo se ha puesto en cola en la unidad de disco duro de Fiery, es posible que permanezcan en la unidad de disco duro elementos del trabajo, con lo que en teoría podrían recuperarse con determinadas herramientas, como por ejemplo las de análisis forense de discos.

6.2.5 Borrado seguro

El Borrado seguro está diseñado para eliminar el contenido de un trabajo enviado desde una unidad de disco duro de Fiery siempre que una función de Fiery elimina un trabajo. En el momento de la eliminación, cada archivo original del trabajo se sobrescribe tres veces mediante un algoritmo basado en la especificación del Departamento de Defensa de los Estados Unidos DoD5220.22M.

Para el Borrado seguro se aplican las siguientes limitaciones y restricciones:

- No se aplica a archivos de trabajo que se encuentren en sistemas que no son el servidor Fiery, como por ejemplo:
  – Copias del trabajo asignadas a otro servidor Fiery para equilibrar la carga.
  – Copias del trabajo archivadas en medios o unidades de red.
  – Copias del trabajo ubicadas en estaciones de trabajo cliente.
  – Páginas de un trabajo fusionadas o copiadas por completo en otro trabajo.
- No elimina ninguna entrada del registro de trabajos.
- Si el sistema se apaga manualmente antes de que haya finalizado la eliminación del trabajo, no existe la garantía de que el trabajo se haya eliminado completamente.
- No elimina ningún dato del trabajo que se haya escrito en el disco tras el intercambio de disco o la escritura en la caché de disco.
- El cliente FTP puede guardar los trabajos enviados mediante el servidor FTP antes de que se transfieran al software del sistema de Fiery. Debido a que el software del sistema de Fiery no controla este proceso, el sistema no puede borrar de forma segura los trabajos guardados por el cliente de FTP.
- Los trabajos impresos mediante SMB se transfieren al spooler del Fiery, que guarda en disco los trabajos. Como el software del sistema Fiery no controla este proceso, el sistema no puede eliminar de forma segura estos trabajos.

Nota: El intercambio de disco se produce para crear más memoria virtual que la que hay como memoria física. Este proceso se realiza a nivel de sistema operativo y el servidor Fiery no tiene ningún control sobre el mismo. No obstante, el espacio de intercambio de disco se reescribe periódicamente durante el funcionamiento del sistema operativo cuando se mueven varios segmentos de memoria entre la memoria y el disco. Este proceso puede provocar que algunos segmentos de trabajo se almacenen de forma temporal en el disco.

6.2.6 Memoria del sistema

El procesamiento de algunos archivos puede escribir algunos datos del trabajo en la memoria del sistema operativo. En algunos casos, puede que esta memoria se almacene en la caché de la unidad de disco duro y no se sobrescriba específicamente.

6.3 Impresión segura

La función Impresión segura exige al usuario introducir una contraseña específica del trabajo en el servidor Fiery para permitir la impresión del trabajo. Esta función requiere una interfaz de LCD local con el servidor Fiery.

El objetivo de esta función es limitar el acceso a un documento a sólo los usuarios que (a) tengan la contraseña para ese trabajo y (b) puedan introducirla localmente en el servidor Fiery.

6.3.1 Flujo de trabajo

El usuario introduce una contraseña en el campo Impresión segura del controlador Fiery. Cuando este trabajo se envía a la cola de Impresión o cola En espera de Fiery, el trabajo se sitúa en la cola y se retiene hasta que se introduzca la contraseña.

Nota: Los trabajos enviados con una contraseña de impresión segura no se pueden visualizar desde Fiery Command WorkStation ni Fiery Command WorkStation ME.

En el LCD de Fiery, el usuario accede a la ventana Impresión segura e introduce una contraseña. A continuación, el usuario puede acceder a los trabajos enviados con esa contraseña e imprimirlos o eliminarlos.

Los trabajos de impresión segura no se mueven a la cola Impresos. El trabajo se elimina automáticamente una vez ha finalizado la impresión.

6.4 Impresión por correo electrónico

El servidor Fiery recibe e imprime trabajos enviados a través de correo electrónico. El administrador puede almacenar una lista de direcciones de correo electrónico autorizadas en el servidor Fiery. Se eliminará todo mensaje recibido de una dirección de correo electrónico que no conste en la lista de direcciones de correo electrónico autorizados. El administrador puede desactivar la función de impresión por correo electrónico. La función de impresión por correo electrónico está desactivada de forma predeterminada.

6.5 Administración de trabajos

Sólo se pueden realizar acciones en los trabajos enviados al servidor Fiery mediante una utilidad de administración de trabajos de Fiery con acceso de administrador u operador. Los usuarios invitados (es decir,
sin contraseña) pueden ver los nombres de archivo y los atributos del trabajo, pero no pueden realizar ninguna acción ni ver una presentación preliminar de dichos trabajos.

6.6 Registro de trabajos

El registro de trabajos se almacena en el servidor Fiery. No es posible eliminar los registros individuales del Registro de trabajos. El registro de trabajos contiene información de la impresión y el escaneado de trabajos, como por ejemplo qué usuario ha iniciado el trabajo, cuándo se ha realizado el trabajo, las características del trabajo en cuanto a papel utilizado, color, etc. El registro de trabajos puede utilizarse para analizar la actividad de trabajos del servidor Fiery.

Un usuario con acceso de operador puede ver, exportar o imprimir el registro de trabajos desde Fiery Command WorkStation. Un usuario con acceso de administrador puede eliminar el registro de trabajos desde Fiery Command WorkStation. Un usuario con acceso de invitado puede imprimir el registro de trabajos desde el LCD de Fiery únicamente si el administrador le ha otorgado ese acceso.

6.7 Configuración

Esta función requiere una contraseña de administrador. El servidor Fiery puede configurarse mediante la herramienta Fiery Configure o el LCD de Fiery. La herramienta Fiery Configure puede iniciarse desde Fiery WebTools y Fiery Command WorkStation.

6.8 Escaneado

El servidor Fiery permite escanear de nuevo una imagen colocada en la ventana de la copiadora a la estación de trabajo desde la que se inició el escaneado mediante el plugin TWAIN de Fiery. Este plugin es compatible con las aplicaciones Adobe® PhotoShop y Textbridge. Cuando una función de escaneado se inicia desde una estación de trabajo, la imagen de mapa de bits en bruto se envía directamente a la estación de trabajo.

El usuario puede escanear documentos al servidor Fiery para su distribución, almacenamiento y recuperación. Todos los documentos escaneados se almacenan en el disco. El administrador puede configurar el servidor Fiery para que elimine automáticamente los trabajos escaneados después de un período de tiempo predefinido.

Los trabajos escaneados pueden distribuirse a través de los métodos siguientes:

- Correo electrónico: En este proceso, el mensaje de correo electrónico se envía a un servidor de correo, desde donde se redirige al destino deseado. Nota: Si el tamaño de archivo es superior al máximo definido por el administrador, el trabajo se almacena en la unidad de disco duro de Fiery, a la que puede accederse mediante un URL.
- FTP: El archivo se envía a un destino de FTP. En el registro de FTP se conserva un registro de la transferencia, incluido el destino, al que se puede acceder con el comando Imprimir páginas del LCD. Se puede definir un servidor proxy FTP para enviar el trabajo a través de un cortafuegos.
- Cola En espera de Fiery: El archivo se envía a la cola En espera de Fiery
(consulte la sección 6.2.1 anterior) y no se conserva como trabajo escaneado.
- Fax de Internet: El archivo se envía a un servidor de correo, desde donde se direcciona al destino de fax por Internet deseado.
- Buzón: El archivo se almacena en el servidor Fiery con un número de código de buzón. El usuario tiene que especificar el código de buzón correcto para poder acceder al trabajo escaneado almacenado. Algunas versiones del servidor Fiery también requieren una contraseña. El registro de trabajos se almacena en el servidor Fiery.

7 Conclusión

EFI ofrece un sólido conjunto de funciones y opciones estándar en el servidor Fiery para ayudar a nuestros clientes a responder a la necesidad de contar con una solución de seguridad completa y personalizable para cualquier entorno. EFI se compromete a garantizar que los negocios de nuestros clientes funcionen con la máxima eficiencia y a proteger de forma eficaz el servidor Fiery frente a vulnerabilidades procedentes de un uso malintencionado o accidental. Por ello, EFI desarrolla continuamente nuevas tecnologías para proporcionar soluciones de seguridad globales y fiables para el servidor Fiery.

TL035.07.18_ES