Fiery FS500 Pro/FS500 servers

Fiery Security White Paper

45234237

3 de julio de 2022

Contenido

Información general del documento

Este documento proporciona información detallada acerca de la implementación de la tecnología y las características de seguridad en Fiery FS500 Pro/FS500 servers y abarca la seguridad del hardware, la seguridad de la red, el control de acceso, los sistemas operativos y la seguridad de datos. La finalidad del documento es ayudar a nuestros clientes a combinar la tecnología de seguridad de la plataforma Fiery con sus propias políticas para cumplir sus requisitos de seguridad específicos.

Convenciones de terminología

Este documento utiliza la siguiente terminología para hacer referencia al Fiery FS500 Pro/FS500 servers , las impresoras y las aplicaciones Fiery.

Término o convención	**Se refiere a**
Fiery server	Fiery FS500 Pro/FS500 servers
Impresora	Impresora, copiadora, imprenta digital, impresora o dispositivo de salida
Configure	Fiery Configure
Command WorkStation	Fiery Command WorkStation
WebTools	Fiery WebTools
QuickTouch	El software Fiery QuickTouch se ejecuta en el panel LCD del servidor Fiery

Filosofía de seguridad de EFI

EFI entiende que la seguridad es una de las mayores preocupaciones para las organizaciones y empresas en el mundo. Nuestros productos se mejoran con frecuencia con funciones de seguridad para proteger sus activos empresariales. Fiery servers de EFI están diseñados y fabricados con la seguridad como componente básico para proteger los datos del sistema en reposo, en tránsito y durante el procesamiento.

Al trabajar estrechamente con nuestros colaboradores y proveedores globales de EFI, estamos comprometidos a apoyar continuamente a nuestros clientes con soluciones a medida que evolucionan las amenazas. Para lograr la seguridad general del sistema, recomendamos a los usuarios finales que combinen las características de seguridad de Fiery con las políticas de seguridad de su propia organización y las mejores prácticas específicas del sector, como, por ejemplo, el uso contraseñas seguras y sólidos procedimientos de seguridad físicos.

Objetivos de seguridad de EFI

EFI ha establecido los siguientes objetivos para implementar las medidas de seguridad para Fiery server:

- **Seguridad de datos**: divulgación no autorizada de datos durante el procesamiento, la transmisión (en tránsito) o el almacenamiento (en reposo).
- **Disponibilidad**: rendimiento tal como está previsto, sin manipulación no autorizada.
- **Control de acceso**: disponibilidad del servicio para los usuarios autorizados.
- **Mantenimiento sencillo desde el punto de vista de las TI**: notificaciones automáticas y descargas cuando hay actualizaciones de seguridad disponibles.
- **Cumplimiento**: compatibilidad con las normativas del sector y los marcos de seguridad.

Actualizaciones de seguridad del software Fiery

En esta sección se proporciona información general sobre el proceso de actualización de seguridad del software del Fiery server. Las vulnerabilidades de seguridad de Microsoft® Windows™ OS no se describen debido a que Microsoft las maneja directamente y se entregan como actualizaciones de Windows cuando están disponibles. En el caso de problemas de seguridad o vulnerabilidades que pueden afectar al núcleo de los componentes de hardware de Fiery, como por ejemplo la placa base, el procesador, BIOS, etc., EFI colabora estrechamente con los fabricantes para obtener las actualizaciones de seguridad requeridas.

- EFI supervisa el boletín semanal de seguridad cibernética de US-CERT de la Agencia de Seguridad Cibernética y de Infraestructuras (CISA). Este boletín proporciona un resumen de las nuevas vulnerabilidades que se han registrado en la base de datos de vulnerabilidades nacionales (NVD) del Instituto Nacional de Normalización y Tecnología (NIST) durante la semana pasada. Las vulnerabilidades se basan en los estándares de denominación de vulnerabilidades y exposiciones comunes (CVE) y se organizan en función de la gravedad (alta, media y baja) determinada por el sistema común de puntuación de vulnerabilidades (CVSS).
- EFI proporciona soluciones de seguridad para cada plataforma Fiery server lo antes posible.
- Las actualizaciones de seguridad del software Fiery se envían a colaboradores específicos de EFI para su aprobación.
- Una vez aprobadas por los colaboradores, las actualizaciones de seguridad del software Fiery pasan a estar disponibles para la descarga.
- La actualización del sistema Fiery descarga e instala las actualizaciones de seguridad si la opción está habilitada en el Fiery server. Por defecto, esta opción está habilitada y se recomienda dejarla activada.

Las actualizaciones oportunas de software son vitales para un funcionamiento óptimo de Fiery servers. La instalación de las actualizaciones de seguridad del software de Fiery y del sistema operativo Windows son importantes para mantener la seguridad de los Fiery servers en un entorno de impresión determinado.

Nota: Todas las actualizaciones o parches de Fiery están firmados digitalmente con SHA-2.

Configuración de las características de seguridad de Fiery server

Configure es la herramienta principal que se utiliza para configurar las características de seguridad de Fiery servers. Los Administradores de Fiery pueden acceder a Configure desde Command WorkStation o WebTools.

Nota: Los usuarios deben disponer de privilegios de administrador para poder acceder a Configure.

Para obtener más información acerca de la configuración de Fiery server, consulte Indicaciones generales para la configuración segura del servidor Fiery en la página 32.

Seguridad del hardware

La seguridad del hardware de Fiery server se centra en evitar la pérdida de datos en caso de apagón y acceso no autorizado a los datos ubicados en un dispositivo de almacenamiento.

Memoria volátil

Los datos escritos en la RAM volátil solo están disponibles mientras el equipo esté encendido. Cuando se desconecta la alimentación, se eliminan todos los datos.

Para obtener más información, consulte la sección de memoria volátil de la tabla en la página 25.

Memoria no volátil y almacenamiento de datos

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

Para obtener más información, consulte la sección de memoria no volátil de la tabla en la página 25.

Memoria Flash

La memoria flash almacena el programa de autodiagnóstico y arranque (BIOS) y algunos datos de configuración del sistema. La memoria flash se programa en fábrica y solo puede volver a programarse mediante la instalación de muestras especiales creadas por EFI. Si la información está dañada o si se elimina, Fiery server no se iniciará.

CMOS

La memoria CMOS con batería se utiliza para almacenar la configuración de máquina de Fiery server. Ninguna parte de esta información se considera confidencial ni privada. Si la memoria CMOS está instalada, los usuarios pueden acceder a estos valores en un servidor basado en Windows 10 IoT Enterprise 2016 o 2019 con el monitor, el teclado y el ratón.

NVRAM

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

Unidad de disco duro y unidad de estado sólido

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 en un área aleatoria de la unidad de disco duro.

Los usuarios pueden eliminar manualmente los datos de imagen y los trabajos de las colas o cualquier otra operación de cola desde Command WorkStation (por ejemplo, la operación de la impresora LCD). Los datos y objetos de la imagen también se pueden eliminar automáticamente mediante el comando **Clear Server** o cuando el número de trabajos impresos sobrepasa los parámetros permitidos. Si deshabilita la cola Impresos, también se eliminarán los trabajos impresos.

Para proteger los datos de imagen del acceso no autorizado, EFI ofrece la función de borrado seguro. Cuando el administrador de Fiery habilita el borrado seguro, el modo de funcionamiento seleccionado se lleva a cabo en el tiempo adecuado para eliminar de forma segura los datos que se borraron del disco duro. Fiery Secure Erase actualmente solo admite unidades de disco duro Para unidades de estado sólido (SSD), consulte con el fabricante las opciones de solución de errores de disco antes de deshacerse de la unidad.

Nota: Para obtener más información acerca del borrado seguro, consulte Borrado seguro en la página 23.

Puertos físicos

El Fiery server puede conectarse a través de puertos externos que se muestran en la siguiente tabla:

Puertos Fiery	Función	Acceso	Control de acceso
Conector Ethernet RJ-45	Conectividad Ethernet	Conexiones de red	Uso del filtrado IP de Fiery para controlar el acceso
Conector de interfaz de impresora	Imprimir y escanear	Dedicado al envío/ recepción a/desde la impresora	N/D
Puerto USB	Conexión de dispositivos USB Instalación del software de sistema	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 puede desactivarse mediante la Política del Grupo Windows. También se puede deshabilitar el almacenamiento USB desde Configure.
Conector de fibra óptica	Conectividad Ethernet de 10 Gb	Conexiones de red	N/D

Interfaz local

En ciertos Fiery servers, el usuario puede acceder a las funciones de Fiery en el monitor del Fiery NX Station, a través del software de Fiery QuickTouch en la pantalla táctil o a través de cualquier monitor conectado al Fiery server. El acceso de seguridad en el Fiery server con Fiery NX Station se controla mediante una contraseña de administrador de Windows. La pantalla táctil ofrece funciones muy limitadas que no suponen ningún riesgo para la seguridad.

Kkit opcional de unidad de disco duro extraíble

Algunos Fiery servers son compatibles con el kit opcional 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 quitar las unidades y colocarlas en una ubicación segura tras apagar el Fiery server.

Para servidores Windows independientes

Los Fiery servers independientes basados en Windows son compatibles con kits opcionales de unidades de disco duro extraíbles. La disponibilidad de este kit opcional para un producto Fiery específico depende de los términos de los contratos de EFI con cada socio individual de Fiery.

Para servidores Fiery XB

Las unidades de disco duro y las unidades de estado sólido se pueden quitar de los servidores Fiery XB. La mayoría de las unidades de disco duro y las unidades de estado sólido se combinan en configuración RAID. Es importante que las unidades vuelvan a su ubicación original para evitar la pérdida de datos y la instalación de un nuevo software del sistema.

Habilitar puertos USB para el uso de dispositivos de almacenamiento

Los puertos USB en Fiery servers permiten las conexiones del ratón, el teclado o el espectrofotómetro, pero evitarán las conexiones a los dispositivos de almacenamiento USB cuando la opción Habilitar almacenamiento USB esté deshabilitada en Configure. Esta opción está habilitada por defecto. Cuando esté deshabilitada, la opción desactiva las características de Fiery que requieren funciones de almacenamiento masivo USB, como, por ejemplo, la copia de seguridad y la restauración.

Seguridad de red

El Fiery server incluye una variedad de características de seguridad de red diseñadas para controlar y administrar el acceso a la impresora. Solo usuarios y grupos autorizados pueden acceder al Fiery server e imprimir en la impresora. Fiery server también puede configurarse para limitar o controlar las comunicaciones externas mediante direcciones IP designadas y al deshabilitar los puertos y protocolos de red. Fiery servers debería estar siempre distribuido en un entorno de red protegido y un administrador de red cualificado y autorizado debe configurar y administrar correctamente la accesibilidad la accesibilidad.

Puertos de red

Por defecto, todos los puertos TCP/IP que no utilizan los servicios Fiery específicos están deshabilitados. El administrador de Fiery puede habilitar y deshabilitar de forma selectiva los puertos de red. Al deshabilitar un puerto de red se bloquean las conexiones externas mediante el puerto especificado. Si un puerto concreto está habilitado, las conexiones externas pueden utilizar dicho puerto.

TCP	UDP	Nombre del puerto	Servicios dependientes
20-21		FTP	FTP
80		HTTP	WebTools, IPP
135		MS RPC	Microsoft® RPC Service (solo Windows 10). 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	Fiery Central, algunas utilidades anteriores y otras herramientas basadas en SNMP
	427	SLP	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 versiones anteriores de Command WorkStation)
631		IPP	IPP

TCP	UDP	Nombre del puerto	Servicios dependientes
3389		RDP	Escritorio remoto (solo servidores Fiery para Windows)
3702	3702	WS-Discovery	WSD
	4500	NAT de IPsec	IPsec
	5353	Multicase DNS	Bonjour
6310 8010 8021-8022 8090 9906 21030 50006-50025	9906	Puertos EFI	Command WorkStation 5 y 6, 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

Nota: Los puertos 50006-50025 están habilitados tras instalar Command WorkStation, versión 6.2 y posteriores en un Fiery server independiente.

Los otros puertos TCP, excepto los especificados por el colaborador de Fiery, 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 Fiery server.

Filtrado de IP

El filtrado de IP permite o niega las peticiones de conexión al Fiery server desde direcciones IP definidas. El administrador puede definir políticas por defecto para permitir o denegar paquetes de datos entrantes y también puede especificar filtros para un máximo de 16 direcciones IP o rangos para, de este modo, permitir o denegar las peticiones de conexión.

Cada configuración de filtro IP especifica una dirección IP o un rango de direcciones IP y la acción correspondiente. Si se Rechaza la acción, se eliminarán los paquetes que tengan una dirección de origen que pertenezca a las direcciones especificadas y, si se Acepta la acción, se admitirán los paquetes.

Autenticación de red

SNMP v3

El Fiery server admite el estándar de SNMPv3 más reciente. Los paquetes de comunicación SNMPv3 pueden encriptarse para garantizar la confidencialidad, la integridad del mensaje y la autenticación.

El administrador de Fiery puede elegir entre tres niveles de seguridad en SNMP: Mínimo, Medio o Máximo. El administrador de Fiery también puede solicitar autenticación antes de permitir transacciones SNMP y encriptar los nombres de usuarios y contraseñas SNMP. El administrador local puede definir los nombres de comunidad de lectura y escritura SNMP, así como otras configuraciones de seguridad.

Para obtener más información, consulte la Configuración recomendada en la página 32.

IEEE 802.1x

802.1x es un protocolo estándar IEEE para control del acceso a la red basado en puertos. Dicho protocolo proporciona un mecanismo de autenticación antes de que Fiery server consiga acceder a la LAN y sus recursos.

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

El Fiery server se autentica al iniciarse o cuando el cable Ethernet se desconecta y vuelve a conectarse.

Encriptación de red

Seguridad del protocolo de Internet (IPsec)

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

El Fiery server utiliza una autenticación 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 equipo cliente y un Fiery server, todas las comunicaciones (incluidos los trabajos de impresión) se transmiten de forma segura a través de la red.

HTTPS

El Fiery server requiere una conexión segura entre clientes y diferentes componentes del servidor. Se utiliza HTTPS a través de TLS para encriptar comunicaciones entre los dos puntos finales. Se necesita HTTPS para conectarse al Fiery server desde WebTools y Fiery API. Estas comunicaciones se encriptan con TLS 1.3 y 1.2.

Gestión de certificados

Los Fiery servers proporcionan una interfaz para administrar los certificados utilizados durante las comunicaciones TLS. Fiery servers admiten el formato de certificado X.509.

Los Fiery servers admiten certificados RSA con longitud de clave de 4096, 3072 y 2048 bits.

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

- Crear certificados digitales autofirmados.
- Añadir un certificado y su clave privada correspondiente para el Fiery server.
- Añadir, examinar, ver y eliminar certificados de una entidad de certificación de confianza.

Nota: Los certificados autofirmados no son seguros. Le recomendamos encarecidamente a los usuarios que utilicen un certificado de una entidad de certificación (CA) de confianza.

Una vez que obtenga un certificado firmado por una entidad de certificación de confianza, puede cargar el certificado en el Fiery server en la sección Configure de WebTools.

Seguridad de correo electrónico

Fiery server admite protocolos de comunicación de correo electrónico PLV y SMTP si está habilitado el correo electrónico. (La función está desactivada por defecto.) Para proteger el servicio frente a ataques o usos inadecuados, el administrador de Fiery puede habilitar otras funciones de seguridad adicionales.

PLV antes de SMTP

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

OP25B

Outbound Port 25 Blocking (OP25B) es una medida antispam 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.

Para obtener más información acerca del flujo de trabajo de impresión de correo electrónico de Fiery server, consulte Impresión de correo electrónico en la página 26.

Server Message Block (SMB)

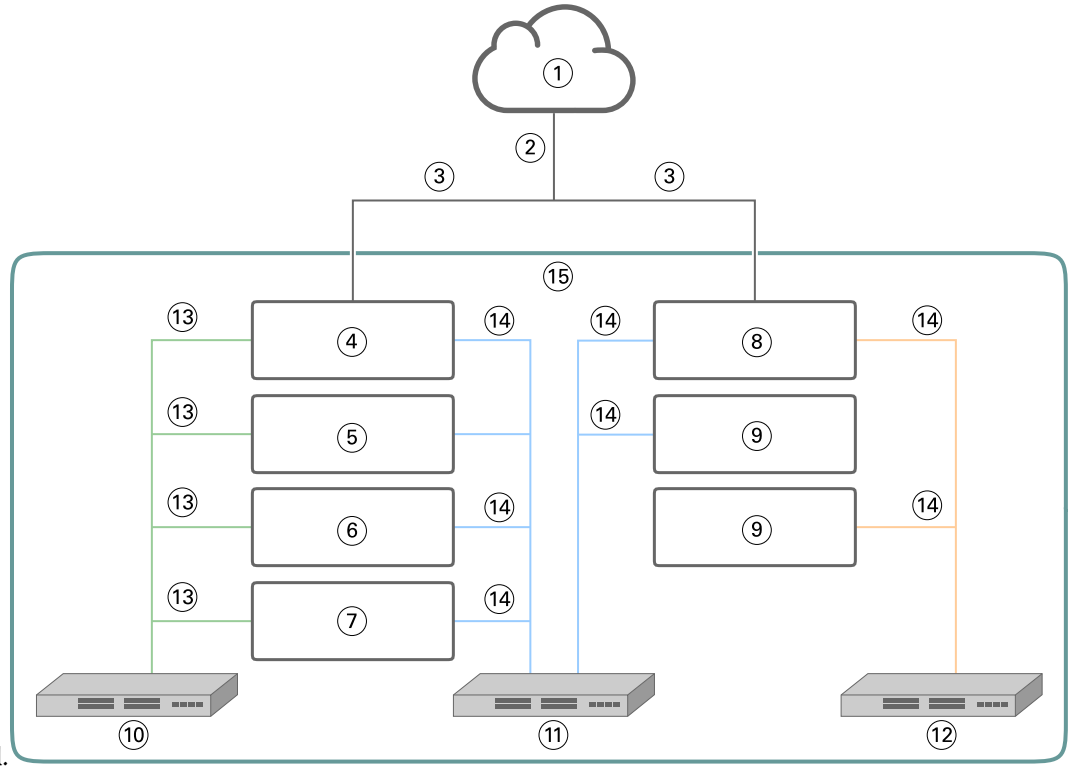
SMB es un protocolo de red que permite el acceso compartido a archivos e impresoras. SMB v1 está deshabilitado en Fiery servers, ya que no cumple los estándares de seguridad actuales del sector. SMB v2 y v3 siguen siendo compatibles.

La firma SMB se aplica en el Fiery server. La firma SMB requiere que los paquetes se firmen digitalmente para permitir al destinatario comprobar la autenticidad del paquete para evitar ataques de intermediarios. Si la autenticación SMB está habilitada, el usuario debe proporcionar el nombre de usuario y la contraseña SMB para acceder a las carpetas SMB y al contenido almacenado en las carpetas SMB.

Nota: La impresión o el uso compartido de archivos a través de SMB puede restringirse estableciendo una contraseña en Configure.

Diagrama de red Fiery XB

El siguiente gráfico muestra cómo se conectan a la red los servidores Fiery XB y las impresoras inkjet de alta velocidad.



1	LAN	9	Otros blades de impresora (opcional)
2	Gestión de trabajos en tráfico de red	10	Red privada de 10 GbE
3	1 GbE DHCP o fija	11	Red privada de 1 GbE
4	Blade principal de Fiery	12	Red privada PLC de 1 GbE
5	Blade de Fiery RIP (opcional)	13	10 GbE
6	Blade de Fiery n.º 1 (opcional)	14	1 GbE
7	Blade de Fiery n.º 2 (opcional)	15	Entorno Fiery XB cerrado
8	Impresora Blade		

Control de acceso

En este capítulo se describe cómo Fiery server puede configurarse para controlar el acceso a los recursos para grupos de usuarios diferentes.

Autenticación del usuario

La función de autenticación de usuario permite al Fiery server hacer lo siguiente:

- Autenticar un usuario
- Autorizar acciones según los privilegios del usuario

El Fiery server puede autenticar usuarios que estén:

- Basados en el dominio: usuarios definidos en un servidor corporativo y que acceden mediante LDAP.
- Basados en Fiery: usuarios definidos en el Fiery server

El Fiery server autoriza las acciones del usuario en función del grupo al que pertenezca. Cada grupo está asociado a 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 dichos privilegios. El administrador de Fiery puede modificar los privilegios de cualquier grupo de Fiery, con la excepción de las cuentas de Administrador y Operador.

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

- **Imprimir en escala de grises**: este privilegio permite a los miembros del grupo imprimir trabajos en escala de grises en el Fiery server . Si el usuario no dispone de este privilegio, el Fiery server no imprimirá el trabajo. Si el trabajo es un trabajo de color, se imprimirá en escala de grises.
- **Imprimir en color y en escala de grises**: este privilegio permite a los miembros del grupo imprimir trabajos en el Fiery server con acceso completo a las funciones de impresión en color y en escala de grises de Fiery server. Si no se dispone de ninguno de los dos privilegios anteriores, el trabajo de impresión no se imprimirá y los usuarios no podrán enviar el trabajo por FTP (solo dispositivos de color).
- **Buzón de Fiery**: este privilegio permite a los miembros del grupo tener buzones individuales. El Fiery server crea un buzón en función del nombre de usuario con un privilegio de buzón. Solo pueden acceder a este buzón los usuarios con el nombre de usuario y la contraseña del buzón.
- **Calibración**: este privilegio permite a los miembros del grupo calibrar el 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.
- **Editar trabajos** (solo servidores Fiery XB): este privilegio permite a los miembros del grupo editar un trabajo en la cola.

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

Autenticación del usuario del software Fiery

Fiery server interactúa con diferentes tipos de usuarios. Estos usuarios son específicos del software Fiery y no están relacionados con usuarios ni funciones definidos en Windows. Se recomienda que los administradores de Fiery requieran contraseñas para el acceso a Fiery server. Además, EFI recomienda que el administrador de Fiery cambie la contraseña por defecto para cumplir los requisitos de seguridad del entorno de impresión del usuario.

- La contraseña máxima permitida para "Administrador" y para "Operador" es de hasta 15 caracteres cuando se utiliza Configure > Seguridad.
- La contraseña máxima permitida para las cuentas de usuarios locales es de hasta 64 caracteres cuando se utiliza Configure > Cuentas de usuario.
- Las contraseñas de Administrador y de Operador también pueden modificarse en Configure > Cuentas de usuario, donde se permite un máximo de 64 caracteres.

A continuación, se describen los privilegios permitidos para los diferentes tipos de usuarios de Fiery:

- **Administrador**: tiene control total sobre todas las funciones de Fiery server.

  El administrador de Fiery puede modificar los privilegios de cualquier grupo de Fiery, con la excepción de las cuentas de Administrador y Operador.
- **Operador**: tiene los mismos privilegios que el administrador, pero no tiene acceso a algunas funciones de Fiery server, como, por ejemplo, la configuración, y no puede eliminar el registro de trabajos.
- **Operador de la impresora** (solo para servidores Fiery): puede administrar los trabajos en la impresora. El administrador puede agregar privilegios específicos a este tipo de usuario.
- **Admin de servicio Fiery** (Fiery servers solo en Windows): se utiliza una cuenta de administrador oculta para instalar el certificado de confianza en los servidores Windows. Esta cuenta no permite a los usuarios iniciar sesión en el Fiery server (local o remoto). Esta cuenta podría aparecer en algunas herramientas de exploración de red y puede eliminarse si es necesario. Se pueden utilizar métodos estándar alternativos para instalar el certificado de confianza.

Registro de auditoría de seguridad de Fiery

Para ayudar a las organizaciones con los requisitos de cumplimiento, los administradores de Fiery pueden recopilar y analizar eventos relacionados con la seguridad, que se guardan en el Registro de auditoría de seguridad.

El Registro de auditoría de seguridad está habilitado por defecto.

Cada evento de seguridad está clasificado como Información, Advertencia o Error. No hay alertas ni notificaciones al administrador, solamente un registro estático.

Los registros están en un formato compatible con las soluciones de recopilación y análisis de registros SIEM comunes. La información acerca de los eventos capturados se ajusta a la publicación especial 800-53 del NIST, *Recommended Security Controls for Federal Information Systems* (SP800-53).

El administrador de Fiery puede leer los eventos sin la intervención de EFI. Los eventos de los Fiery servers tanto de Windows como de Linux, están en formato JSON y pueden ser procesados por cualquier herramienta de recopilación de registros. En el caso de los servidores Fiery de Windows, los eventos pueden visualizarse en el Administrador de eventos de Windows. Los administradores de los Fiery servers de Linux pueden reenviar registros a un sistema central de recopilación de registros (SysLog).

Los eventos de seguridad se conservan según la capacidad de almacenamiento en disco que se haya asignado. Cuando el tamaño del registro alcanza el límite máximo de almacenamiento (400 MB), se eliminan los eventos más antiguos.

Sistemas operativos

EFI colabora estrechamente con los fabricantes de los sistemas operativos utilizados en Fiery servers para obtener las actualizaciones de seguridad necesarias para resolver los problemas de seguridad o vulnerabilidades que pueden afectar al núcleo de los componentes de Fiery server, como, por ejemplo la placa base, el procesador, la BIOS, etc. Además, las actualizaciones de software Fiery se han firmado digitalmente por EFI para evitar modificaciones no autorizadas, incluida la inserción de malware.

Linux (FS500)

Los Fiery servers FS500 son servidores basados en Linux diseñados con arquitectura cerrada. La visibilidad limitada de la red impide el acceso no autorizado.

Las características de Linux son las Fiery servers siguientes:

- Los Fiery servers basados en Linux no incluyen una interfaz local que permita el acceso al sistema operativo.
- SSH y Telnet no son compatibles con Fiery servers basados en Linux, lo que impide el acceso al shell del sistema operativo.
- Fiery servers basado en Linux impide la instalación de programas no autorizados que podrían exponer el sistema a vulnerabilidades.
- El sistema operativo Linux utilizado en los Fiery servers FS500 es un sistema operativo personalizado solo para Fiery servers. Tiene todos los componentes del sistema operativo que requiere un Fiery server, pero no ciertos componentes de uso general y aplicaciones para el usuario final que se encuentran comúnmente en los sistemas Linux.

Acceso al sistema

Basado en Linux, Fiery servers puede configurarse a través de la configuración de Fiery, en el panel de control de la impresora o a través de Configure en WebTools. WebTools es un conjunto de páginas basadas en un navegador que permite al Administrador de Fiery acceder al Fiery server para la configuración y otras actividades relacionadas con la administración del sistema. WebTools funciona con la última estructura web fiable, que es compatible con la mayoría de navegadores web actuales.

Windows 10 (FS500 Pro)

Los Fiery servers FS500 Pro independientes utilizan Windows 10 IoT Enterprise 2019 LTSC como sistema operativo propio. Esta versión de Windows contiene la protección de seguridad más reciente e incluye las mejoras acumulativas de Windows 10 de las versiones 1703, 1709, 1803 y 1809. Microsoft es compatible con las actualizaciones de seguridad de cada LTSC Build hasta diez años después del lanzamiento.

Nota: Windows 10 IoT Enterprise 2019 LTSC es un equivalente binario a Windows 10 Enterprise, versión 1809.

Windows 10 IoT Enterprise 2019 LTSC incluye las siguientes funciones:

- Previsto para el uso en sistemas especializados como Fiery servers.
- Incluye numerosas mejoras de seguridad frente a amenazas, información y protección de identidad
- Ofrece numerosas actualizaciones de seguridad.
- No incluye aplicaciones orientadas al consumidor como, por ejemplo, Calendario, Tiempo, Fotos y otros.

Microsoft Windows Update

Microsoft emite periódicamente parches de seguridad a través de Windows Update para abordar las posibles vulnerabilidades y amenazas de seguridad del sistema operativo. La configuración por defecto de Windows Update en Fiery servers notifica al usuario sobre los parches pero sin descargarlos. Si selecciona Buscar actualizaciones en Windows Update en el Panel de control de Windows, se activarán las actualizaciones automáticas y se iniciará el proceso de actualización.

Herramientas de actualización de Windows

El Fiery servers basado en Windows utiliza métodos estándar de Microsoft para actualizar todos los parches de seguridad de Microsoft aplicables. El Fiery server no admite ninguna otra herramienta de actualización de otros fabricantes para recuperar los parches de seguridad.

Software antivirus para Windows

Fiery servers utilizan el software antivirus de Microsoft y Windows 10 Defender para su protección. En general, puede utilizar software antivirus de terceros con un Fiery server. El software antivirus se suministra de muchas formas diferentes y puede contener muchos componentes y funciones para solucionar un riesgo.

Tenga en cuenta que el software antivirus es más útil y seguro cuando se instala, configura y ejecuta en el Fiery server. Para los Fiery servers sin configuración local, es posible ejecutar un software antivirus en un equipo remoto y analizar una unidad de disco duro de Fiery server compartida. Sin embargo, EFI recomienda que el administrador de Fiery colabore directamente con el fabricante del software antivirus para obtener asistencia si lo necesita.

Mecanismo de análisis antivirus

El análisis de Fiery server con un mecanismo de análisis antivirus puede afectar al rendimiento de Fiery, aunque el análisis se haya programado.

Antispyware

La utilización de programas antispyware puede afectar al rendimiento cuando se están importando archivos a Fiery server. Por ejemplo: trabajos de impresión entrantes, archivos que se descargan durante la actualización del Fiery server o una actualización automática de aplicaciones que se ejecutan en el Fiery server.

Firewall integrado

Dado que el Fiery server cuenta con un firewall integrado, no es necesario instalar programas de este tipo. EFI recomienda que los clientes trabajen con su propio departamento de TI si necesitan instalar y ejecutar un firewall integrado que forme parte del software antivirus. Consulte Puertos de red en la página 11 para la lista de puertos disponibles.

Antispam
Fiery server es compatible con las características de impresión por correo electrónico y escaneado en correo electrónico. Se recomienda utilizar un mecanismo de filtrado de spam basado en servidor. Fiery servers también puede configurarse para imprimir documentos desde direcciones de correo electrónico determinadas. No se necesita el componente antispam porque la ejecución de un cliente de correo electrónico separado (como, por ejemplo, Outlook) en Fiery server no es una operación admitida.

HIPS y control de aplicaciones
Debido a la naturaleza compleja del Sistema de Prevención de Intrusiones basado en Host (HIPS) y al control de aplicaciones, la configuración antivirus debe ser probarse y confirmarse de manera exhaustiva si se utiliza alguna de estas características. Cuando están ajustadas correctamente, HIPS y el control de aplicaciones son excelentes medidas de seguridad y pueden coexistir con el Fiery server. Sin embargo, es fácil provocar problemas en Fiery server si se utilizan valores incorrectos de parámetros de HIPS y exclusiones de archivos incorrectas, causadas muchas veces por "aceptar los valores predeterminados". La solución es revisar las opciones seleccionadas en los valores de HIPS y el control de aplicaciones junto con la configuración del Fiery server, como, por ejemplo, puertos de red, protocolos de red, ejecutables de aplicaciones, archivos de configuración, archivos temporales, etcétera.

Lista segura y lista bloqueada
Las funciones de las listas seguras y las listas bloqueadas no suelen tener efectos negativos en el Fiery server. EFI recomienda encarecidamente que el cliente configure estas funciones para no bloquear los módulos Fiery.

Virus de correo electrónico

Normalmente, los virus que se transmiten a través del correo electrónico requieren algún tipo de ejecución por parte del destinatario. Fiery server descarta los archivos adjuntos que no son archivos PDL. Fiery server también ignora el correo electrónico en formato RTF o HTML, o el código 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.

Nota: Para obtener más información acerca del flujo de trabajo de impresión de correo electrónico de Fiery server, consulte Impresión de correo electrónico en la página 26.

Seguridad de datos

Esta sección describe los controles de seguridad diseñados para proteger los datos de usuario contenidos en Fiery server y los controles de seguridad para los datos en tránsito.

Encriptación de información crítica

La encriptación de información crítica en Fiery server garantiza que todas las contraseñas y la información de configuración relacionada sean seguras cuando se almacenan en Fiery server. La información crítica está encriptada o con hash. Los algoritmos criptográficos utilizados son AES256, Diffie-Hellman y SHA-2 para cumplir los estándares de seguridad más recientes.

La información del usuario almacenada en el disco no se podrá leer si se quita el disco de Fiery server. La encriptación de datos del usuario puede habilitarse o deshabilitarse en Fiery servers basados en Windows mediante Configure. En Fiery servers con Linux, esta característica siempre está habilitada.

Si se olvida la contraseña que debe introducirse para la recuperación de los datos, no existe ninguna forma de restablecerla y EFI no puede recuperarla. En este caso, el software deberá volver a instalarse.

Nota: Con la encriptación de datos, se crean particiones en el disco y solo se encripta la partición de datos del usuario. Las particiones del sistema operativo no se pueden encriptar.

Estándar de codificación avanzada (AES)

Fiery server protege los datos en reposo contra el acceso no autorizado. Además, encripta los trabajos, las imágenes y los datos del cliente con el algoritmo AES de 256 bits.

AES es un estándar de encriptación de tamaño reducido, rápido y difícil de descifrar apto para un amplio rango de dispositivos y aplicaciones. Proporciona un nivel de protección adicional contra el robo de datos a la vez que cumple con las políticas de seguridad corporativas.

Impresión estándar

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

- 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 de impresión y directa para limitar la impresión automática.

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 server. Los trabajos que se envían 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, por ejemplo, Command WorkStation.

La cola Impresión secuencial permite al Fiery server mantener el orden de los trabajos de trabajos concretos que se enviaron desde la red. El flujo de trabajo será de tipo FIFO (orden de llegada), 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 que se envían a través de Fiery server pueden perder el orden debido a muchos factores, como por ejemplo, que el Fiery server permita que se adelanten trabajos más pequeños, mientras que los trabajos más grandes se quedan en la cola.

Cola Impresos

Los trabajos que se envían a la cola Impresión se almacenan en la cola Impresos en el Fiery server después la impresión si la cola Impresos 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 la impresión.

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 Fiery servers.

EFI no recomienda la impresión en la cola directa. Fiery server 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 (impresión de datos variables), 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.

Eliminación de trabajos

No es posible ver ni recuperar un trabajo si se elimina automáticamente del Fiery server o si se borra mediante herramientas Fiery. Si el trabajo se ha puesto en cola en la unidad de disco duro de Fiery server, 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.

Borrado seguro

El borrado seguro está diseñado para eliminar el contenido de un trabajo que se envió desde una unidad de disco duro de Fiery server siempre que una función de Fiery elimina un trabajo. Cuando se elimina un trabajo, cada

archivo original del trabajo se sobrescribe tres veces mediante un algoritmo basado en el método de borrado de datos US DoD 5220,22-M.

Flujos de trabajo	Borrado seguro
Trabajos almacenados en la unidad de disco duro de Fiery server; borrado seguro configurado como Encendido	Sí
Trabajos almacenados en la unidad de disco duro de Fiery server; borrado seguro configurado como Apagado	No
Trabajos recibidos en Fiery server y eliminados tras configurar el borrado seguro como Encendido	Sí
Trabajos recibidos en Fiery server y eliminados antes de configurar el borrado seguro como Encendido	No
Copias del trabajo enviadas a otro Fiery server (reparto de carga)	No
Trabajos archivados en medios extraíbles	No
Trabajos archivados en unidades de red	No
Trabajos ubicados en dispositivos cliente	No
Ejecución de Borrar servidor	Sí
Las páginas se combinaron o copiaron en otro trabajo (por ejemplo, trabajos de Fiery Impose o archivos PDF combinados)	No
Trabajos recibidos de la conexión SMB y guardados en la unidad de disco duro de Fiery server	No
Partes de un trabajo escritas en la unidad de disco duro de Fiery server durante el intercambio de discos u operaciones de almacenamiento en caché	No
Entradas del registro de trabajos	No
Entradas del registro de trabajos después de la ejecución de la función Borrar servidor	Sí
Fiery server desactivado antes de que se complete la eliminación del trabajo	No
Desfragmentación de la unidad de disco duro de Fiery server antes de eliminar un trabajo	No

Nota: La característica de borrado seguro no es compatible con las plataformas de Fiery XB ni con Fiery servers con SSD.

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 cambie a la unidad de disco duro y no se sobrescriba específicamente.

Memoria volátil			
Tipo (SRAM, DRAM, etc.)	**Modificable por el usuario (sí o no)**	**Función o uso**	**Proceso para la corrección**
DRAM	Sí	Memoria principal del sistema (recibe los trabajos que se enviaron a la cola directa)	Apagado Fiery server
SDRAM (en la tarjeta de vídeo)	Sí	Memoria de vídeo	Apagado Fiery server

Memoria no volátil			
Tipo (SRAM, DRAM, etc.)	**Modificable por el usuario (sí o no)**	**Función o uso**	**Proceso para la corrección**
BIOS	No	Funciones de la BIOS	Quitar del enchufe y destruir, pero el sistema dejará de funcionar.
EPROM Ethernet	No	Firmware de chip Ethernet	Desoldar y destruir, pero el sistema dejará de funcionar.
CMOS NVRAM	No	Configuración de almacenamiento de la BIOS	Quite la pila del sistema durante 30 segundos.
Disco duro (HDD) o unidad de estado sólido (SSD)	Sí	Sistema operativo Aplicaciones de Fiery (posiblemente con datos del usuario) Software de sistema Fiery Imprimir trabajos, escanear trabajos y otros datos de usuario Imagen de copia de seguridad por defecto de fábrica	Reinstale el software del sistema. La mayoría de los trabajos se pueden eliminar con la característica de borrado seguro*. Se pueden utilizar herramientas de corrección de terceros y socios de Fiery para completar el borrado de datos de estos dispositivos.

Memoria no volátil			
Tipo (SRAM, DRAM, etc.)	**Modificable por el usuario (sí o no)**	**Función o uso**	**Proceso para la corrección**
Nota: La memoria volátil y la RAM podrían contener datos del cliente al procesar los datos de los clientes. No se almacenan datos de cliente en la memoria no volátil como, por ejemplo, datos de BIOS, CMOS y NVRAM. *Las unidades de estado sólido no pueden corregirse completamente mediante métodos de sobrescritura de múltiples pasadas de borrado seguro debido a la correlación de desgaste de la memoria. Además, los intentos de hacerlo también reducen de forma considerable la vida útil operativa de la unidad de estado sólido. Esta característica no es compatible en las plataformas de Fiery XB.			

Impresión segura

La función Impresión segura exige al usuario introducir una contraseña específica del trabajo en el Fiery server y en la impresora para permitir la impresión del trabajo.

Esta función requiere acceso al el panel de control de la impresora. El propósito de esta función es limitar el acceso a los documentos a usuarios que tengan la contraseña para el trabajo y puedan introducirla localmente en el panel de control de la impresora.

Flujo de trabajo de impresión segura

El usuario introduce una contraseña en el campo Impresión segura del controlador Fiery. Cuando este trabajo se envía a la cola Impresión o cola En espera de Fiery server, 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 Command WorkStation.

En el panel de control de la impresora, el usuario accede a una ventana de impresión segura e introduce una contraseña. A continuación, el usuario puede localizar los trabajos enviados con dicha contraseña, imprimirlos y después eliminarlos.

Los trabajos de impresión segura no se mueven a la cola Impresos y se eliminan automáticamente después de la impresión.

Nota: Parte de los datos pueden permanecer temporalmente en los archivos del sistema operativo.

Impresión de correo electrónico

El Fiery server recibe e imprime trabajos enviados a través de correo electrónico. El administrador puede almacenar en Fiery server una lista con las direcciones de correo electrónico autorizadas. De este modo, se eliminarán los mensajes recibidos de direcciones de correo electrónico que no consten en la lista de direcciones de correo electrónico autorizadas. La función de impresión por correo electrónico está desactivada por defecto. El administrador puede activar y desactivar la función de impresión por correo electrónico.

Gestión de trabajos

Si realiza acciones de trabajo en los trabajos enviados al Fiery server, necesitará una utilidad de gestión del trabajo de Fiery con acceso del administrador o del operador.

Registro de trabajos

El registro de trabajos se almacena en el Fiery server. 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, el usuario que ha iniciado el trabajo, cuándo se ha realizado el trabajo o las características del trabajo en cuanto a papel utilizado, color, etc. El registro de trabajos puede utilizarse para analizar la actividad de trabajos del Fiery server.

Un usuario con acceso de operador puede ver, exportar o imprimir el registro de trabajos desde Command WorkStation. Un usuario con acceso de administrador puede eliminar el registro de trabajos desde Command WorkStation.

Configuración

Esta función requiere una contraseña de administrador. El Fiery server puede configurarse desde la herramienta Configure en WebTools o Command WorkStation, o desde la característica de configuración del Panel de control de la impresora.

Escanear

El Fiery server permite escanear de nuevo una imagen colocada en el cristal de la impresora a la estación de trabajo desde la que se inició el escaneado. 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 Fiery server para su distribución, almacenamiento y recuperación. Todos los documentos escaneados se almacenan en el disco. El administrador puede configurar el Fiery server para que elimine automáticamente los trabajos escaneados después de un período de tiempo predefinido.

Distribución de trabajos escaneados

Los trabajos de escaneado se pueden distribuir con diferentes métodos.

Correo electrónico

Es posible enviar un correo electrónico con un archivo adjunto del trabajo escaneado a un servidor de correo electrónico, donde se encamina al destino deseado.

Nota: Si el tamaño del archivo del trabajo escaneado es superior al máximo definido por el administrador, el trabajo se almacenará en la unidad de disco duro de Fiery server, a la que puede accederse a través de 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 desde el comando Imprimir páginas del panel de control de la impresora. Es posible definir un servidor proxy FTP para enviar el trabajo a través de un cortafuegos.

Cola En espera de Fiery server

El archivo se envía a la cola en espera del Fiery server y no se conserva como trabajo de escaneado.

Para obtener más información acerca de la cola En espera de Fiery server, consulte Colas En espera, Impresión e Impresión secuencial en la página 23.

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 Fiery server con un número de código de buzón. Los usuarios tienen que especificar el código de buzón correcto para poder acceder al trabajo de escaneado almacenado. Los usuarios tienen la opción de configurar contraseñas para proteger el contenido de sus buzones de exploración frente al acceso no autorizado. El trabajo escaneado se puede recuperar a través de una URL.

Cumplimiento de marcos y normativas

En la siguiente tabla se proporciona el cumplimiento de marcos y normativas para servidores Fiery que ejecuten el software del sistema FS500 Pro/FS500.

Marcos / Normativas	Ámbito	Serie NX (FS500 Pro)	Serie A/E (FS500)
FIPS 140-2	• Gobierno de EE.UU. (federal y estatal) • Requisitos de seguridad para módulos criptográficos	En cumplimiento Windows 10 2019 LTSC Certificados FIPS: • #3197 • #3196 • #3092	No cumple
Referentes de CIS	• Global • Sector gubernamental / privado • Líneas base de configuración y prácticas recomendadas para configurar un sistema de forma segura	En cumplimiento Referente de Microsoft Windows 10 Enterprise (versión 1809)	N/D*
Guía de implementación técnica de seguridad (STIG)	• El estándar de configuración del gobierno de EE.UU. (federal y estatal) consta de requisitos de ciberseguridad para un producto específico	Cumplimiento parcial Windows 10 STIG versión 2, R3 Excepciones: CCI-000366: el Módulo de plataforma segura (TPM) no está disponible	N/D*

Marcos / Normativas	Ámbito	Serie NX (FS500 Pro)	Serie A/E (FS500)
ISO/IEC-15408	• Global • Criterios comunes • Criterios de evaluación de técnicas de seguridad de la tecnología de la información para la seguridad de TI	Cumplimiento parcial • Requiere autentificación LDAP/AD para el control de acceso • TPM y arranque seguro no son compatibles	No cumple
IEEE 2600.2-2009	• Global • Sector gubernamental / privado • Perfil de criterios comunes para dispositivos de copias impresas en papel Entorno B	Cumplimiento parcial • TPM y arranque seguro no son compatibles • Los requisitos de resistencia y detección necesitan un kit opcional de seguridad de la unidad de disco Fiery	No cumple
Proteger la matriz de evaluación de seguridad informática (SCSEM)	• Gobierno de EE.UU. (federal y estatal) • Indicaciones generales de seguridad de la información tributaria para organismos federales, estatales y locales	Cumplimiento parcial • TPM y arranque seguro no son compatibles • Los requisitos de resistencia y detección necesitan un kit opcional de seguridad de la unidad de disco Fiery	No cumple
DoD 522.22-M	Estándar de saneamiento de datos. 3 pasadas.	En cumplimiento	En cumplimiento
NIST 800-88	Estándar de saneamiento de datos. 1 pasada.	No cumple	No cumple
Certificación RMF del ejército	• Gobierno de EE.UU. • Marco de gestión de riesgos para la tecnología de la información del ejército	Cumplimiento parcial • TPM y arranque seguro no son compatibles	Cumplimiento parcial • TPM y arranque seguro no son compatibles

* Fuera del ámbito de la normativa o del marco. Los servidores basados en Linux de la serie A y E son sistemas cerrados sin acceso directo al sistema de archivos. La visibilidad limitada de la red impide el acceso no autorizado.

Cumplimiento de FIPS 140-2

Cuando se configuran correctamente, los servidores Fiery que ejecutan FS500 Pro en Windows 10 2019 LTSC cumplen las instrucciones de cifrado de datos de FIPS 140-2. Un servidor Fiery en *Modo FIPS 140-2* utiliza únicamente algoritmos criptográficos validados y certificados en el Programa de Validación de Algoritmos Criptográficos (CAVP) del gobierno federal de EE.UU. para cifrar los datos en reposo y en tránsito.

Habilitar el *Modo FIPS 140-2* en Fiery requiere que el usuario siga un proceso de configuración avanzada para endurecer el servidor.

Indicaciones generales para la configuración segura del servidor Fiery

Las siguientes indicaciones generales pueden ayudar a los administradores de Fiery a mejorar la seguridad al configurar Fiery server.

Cambio de la contraseña de administrador

Se recomienda cambiar la contraseña de administrador Fiery por defecto tras la instalación y de manera periódica según las políticas de seguridad de su organización. La contraseña de administrador por defecto debe cambiarse en el Asistente para la configuración del Fiery durante la primera configuración. Las contraseñas de Administrador y de Operador pueden modificarse después de la primera configuración en WebTools: Configure > Seguridad > Contraseña de administrador (o Contraseña de operador, respectivamente). La configuración de contraseña también está disponible en Cuentas de usuario.

La contraseña de administrador proporciona acceso total al Fiery server de forma local y/o desde un cliente remoto. El acceso total incluye, entre otros:

- Sistema de archivos
- Política de seguridad del sistema
- Entradas del registro
- Contraseña de administrador, que impide el acceso al Fiery server a los usuarios anónimos

Configuraciones recomendadas

- Seleccione el nivel de seguridad Máximo para SNMP en Red > SNMP:

  Si se elige la seguridad máxima, se restringe la compatibilidad de Fiery server solo con SNMP v3.

  Si el responsable del SNMP solo funciona con SNMP v1/v2c, cambie el valor del campo Nombre de comunidad de lectura. El Fiery server le permite cambiar los valores de SNMP de los campos Nombre de comunidad de lectura y Nombre de comunidad de escritura desde WebTools (Configure > Red > SNMP) y desde el panel de control de la impresora (Red > SNMP).
- Deshabilite WSD en el envío de trabajos.
- Deshabilite la impresión en Windows en el envío de trabajos si utiliza LPR, el puerto 9100 o IPP para la impresión.
- Bloquee los puertos habilitando el filtro del puerto TCP/IP en filtrado de puertos Seguridad > TCP/IP.

  Borre los puertos 137-139 y 445 si no utiliza impresión en Windows y no necesita acceder a carpetas de archivo ni compartirlas. Deshabilite las comunicaciones del puerto 80 (HTTP) no seguras.

Además de los niveles de protección del sistema operativo, Fiery server tiene las siguientes características de seguridad adicionales para proteger sus datos:

- Fiery servers disponen de impresión segura para garantizar que el usuario solo recoge su trabajo de impresión.
- Fiery servers están integrados con las soluciones de contabilidad de trabajos principales para incluir seguridad adicional a través de impresión "follow me" (sígueme).

Fiery servers cuentan con numerosas características de seguridad pero no son servidores con acceso a Internet. Deben colocarse en un entorno protegido y el administrador de red debe configurar su accesibilidad de manera adecuada.

Selección de un perfil de seguridad Alto

Fiery server ofrece recomendaciones de seguridad predefinidas en función de los diferentes tipos de riesgos y niveles de amenazas (Estándar, Alto, Actual). Esta función se denomina Perfiles de seguridad y está disponible desde las ubicaciones siguientes:

- Asistente de software Fiery
- WebTools > Configure > Seguridad

El perfil de seguridad Alto permite que el Fiery server sea aún más seguro y habilita las características de seguridad que se utilizan con más frecuencia.

Opción	Alto
Filtrado de puertos TCP/IP	Habilitado
Protocolo Service Location Protocol (SLP)	Deshabilitado
Bonjour	Deshabilitado
Borrado seguro	Habilitado
Escritorio remoto	Deshabilitado
Contraseña SMB	Habilitado
Dispositivos de almacenamiento USB	Deshabilitado
Seguridad PostScript	Habilitado
Puerto 9100	Deshabilitado
LPD	Habilitado
Impresión en Windows	Deshabilitado
IPP	Habilitado
Web Services for Devices (WSD)	Deshabilitado
Imprimir a través de correo electrónico	Deshabilitado
Impresión por FTP	Deshabilitado

Opción	Alto
Impresión móvil directa	Deshabilitado

EFI recomienda utilizar el perfil de seguridad Alto para entornos con requisitos de seguridad máximos.

Conclusión

EFI ofrece un sólido conjunto de funciones de seguridad estándar y opcionales en Fiery server para proporcionar a nuestros clientes soluciones de seguridad completas y personalizables para cualquier entorno. EFI tiene el compromiso de asegurar que el Fiery server está efectivamente protegido contra vulnerabilidades derivadas del uso malicioso o no intencionado para que nuestros clientes puedan gestionar sus empresas con la máxima eficiencia.