Fiery FS800 Pro/FS800 DFEs

Security White Paper

45271120

6 de agosto de 2026

Contenido

Introducción

Este documento ofrece información general sobre las características de seguridad de los servidores de impresión Fiery. Dota a los administradores de tecnología de la información y a los profesionales de la seguridad de la información necesaria para evaluar cómo protegen y protegen los entornos de impresión los servidores de impresión de Fiery. El documento explica los principios y mecanismos utilizados en los servidores de impresión Fiery para proteger los datos, mejorar la seguridad de la red y mantener la integridad del sistema.

Principios de seguridad

Los servidores de impresión Fiery están meticulosamente diseñados para cumplir con las mejores prácticas de la industria, lo que garantiza el cumplimiento de las regulaciones de protección de datos y los requisitos de seguridad empresarial. Los principios fundamentales en los que se basa este diseño son los siguientes:

- Protección de datos: cifrado de datos en reposo y datos en tránsito
- Seguridad de red: acceso controlado, protocolos de comunicación seguros y mecanismos de autenticación
- Integridad del sistema: verificación de firmware, arranque seguro y actualizaciones de seguridad

En colaboración con nuestros colaboradores y proveedores globales, brindamos soporte continuo a nuestros clientes a medida que evolucionan las amenazas. Para garantizar una seguridad integral del sistema, recomendamos a los usuarios finales que integren las características de seguridad de Fiery con las políticas de seguridad de su propia organización y se adhieran a las mejores prácticas del sector, incluyendo la implementación de contraseñas seguras y medidas de seguridad físicas sólidas.

Autenticación y control de acceso

Los servidores de impresión Fiery admiten varios métodos de autentificación, los cuales incluyen:

- Integración LDAP/Active Directory
- La implementación de Autentificación multifactor (MFA) mediante inicio de sesión único (SSO)

Autenticación del usuario

La función de autentificación permite al Fiery DFE realizar las siguientes funciones:

- Autenticar un usuario
- Control de acceso basado en roles (RBAC)

El Fiery DFE admite tres métodos de autentificación de usuario:

- Autentificación local para usuarios definidos en el Fiery DFE
- Autentificación de factor único (SFA) mediante servidores de autentificación de red externos que utilizan LDAP (por ejemplo, Microsoft Active Directory)
- Autentificación multifactor (MFA) mediante inicio de sesión único (SSO)

Independientemente del método utilizado, las cuentas de administrador siempre requieren autentificación. Esto no se puede deshabilitar.

Privilegios de grupo

El Fiery DFE autoriza las acciones en función del grupo al cual pertenece el usuario. Cada grupo está asociado a un conjunto específico de privilegios, como la impresión en color o en escala de blanco y negro. Las acciones de los miembros del grupo están restringidas a estos privilegios. El administrador de Fiery tiene la autoridad para modificar los privilegios de cualquier grupo de Fiery, con la excepción de las cuentas de administrador y operador.

En este método de autenticación de usuario, pueden seleccionarse los diferentes niveles de privilegios de un grupo como se indica a continuación:

- Impresión en blanco y negro: permite a los miembros del grupo imprimir trabajos en blanco y negro. Si el trabajo es un trabajo de color, se imprimirá en blanco y negro.
- Imprimir en color y en blanco y negro: permite a los miembros del grupo imprimir trabajos con acceso completo a las funciones de impresión en color y escala de grises del Fiery DFE. Sin esto o sin el privilegio de imprimir en blanco y negro, los usuarios pueden enviar el trabajo de impresión, pero la impresión fallará.
- Buzón de Fiery: permite a los miembros del grupo tener buzones individuales. El Fiery DFE 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 de servidor: permite a los miembros del grupo crear valores predefinidos de servidor. Los miembros del grupo tienen acceso a estos valores predefinidos de servidor.
- Administrar flujos de trabajo: este privilegio permite a los miembros del grupo crear, publicar o editar impresoras virtuales.
- Editar trabajos (solo servidores de impresión Fiery XB): este privilegio permite a los miembros del grupo editar un trabajo en la cola.

Los administradores con privilegios elevados pueden personalizar estas características para restringir el acceso no autorizado y aplicar los protocolos de seguridad de la organización.

Usuarios locales

El software del Fiery DFEinteractúa con tipos de usuarios únicos, distintos de los usuarios o funciones de Windows. Los administradores de Fiery deberán modificar rápidamente todas las contraseñas predeterminadas tras la instalación inicial. El acceso con contraseña al Fiery DFEdebe aplicarse estrictamente.

- La contraseña máxima para "Administrador" y para "Operador" es de 64 caracteres cuando se utiliza **Configure** > **Seguridad**.
- La contraseña máxima para las cuentas de usuarios locales es de 64 caracteres cuando se utiliza **Configure** > **Cuentas de usuario**.
- Las contraseñas de Administrador y de Operador pueden modificarse en **Configure** > **Cuentas de usuario**.

Cuentas de usuario locales de Fiery y privilegios de acceso:

- Administrador: Control total sobre la funcionalidad del Fiery DFE, puede modificar los privilegios del grupo Fiery, excepto las cuentas de administrador y operador.
- Operador: Tiene los mismos privilegios que el administrador, pero carece de acceso a la configuración del servidor de impresión ni a la eliminación del registro de trabajos.
- Operador de la impresora (solo para servidores de impresión Fiery XB): administra los trabajos en la impresora, con privilegios específicos agregados por el administrador.
- Administrador de Fiery DFE (solo servidores Windows): una cuenta de administrador oculta para instalar el certificado de confianza, no puede iniciar sesión en el Fiery DFE, aparece en las herramientas de exploración de red y se puede eliminar.
- Fiery_SMB_User: Cuenta de impresión de Windows (SMB) por defecto que proporciona visibilidad de las colas de impresión del Fiery DFE a través del entorno de red.
- Invitado (predeterminado, sin contraseña): tiene los mismos privilegios que el operador, pero no puede acceder a los registros de trabajos, realizar modificaciones, cambiar el estado ni obtener una vista previa de los trabajos.

Autentificación LDAP

El Fiery DFE utiliza LDAP versión 3 (compatible con RFC 2251) para comunicarse con los servidores corporativos. A través de LDAPv3, recupera las direcciones de correo electrónico de los usuarios para las características de escaneo,

así como la información de usuarios y grupos para la autenticación. Esta función es exclusiva para conexiones LDAP para los servidores Active Directory.

El Fiery DFE admite los siguientes métodos de autentificación utilizando LDAP:

- Automática
- SIMPLE
- GSSAPI

En la siguiente tabla se describen los distintos métodos de autentificación LDAP:

Método de autentificación	**Descripción**	**Servidor de Active Directory**
Automática	Esta opción selecciona GSSAPI o SIMPLE en función del método de autentificación admitido por el servidor LDAP.	Compatible
SIMPLE	La contraseña es obligatoria. Si se selecciona LDAP a través de TLS, la contraseña se cifra mediante TLS.	Compatible
GSSAPI	Este método utiliza vales Kerberos en lugar de contraseñas, lo que elimina la necesidad de TLS.	Compatible

Inicio de sesión único (SSO)

Los servidores de impresión Fiery FS800 Pro admiten el protocolo OpenID Connect para la autenticación de usuarios de inicio de sesión único (SSO) basada en la nube con Microsoft Entra ID (antes denominado Azure AD). Los usuarios pueden iniciar sesión en un Fiery DFE utilizando sus credenciales Entra ID existentes.

Este método de autentificación es compatible con la autentificación multifactor (MFA).

Este enfoque de gestión de identidades garantiza que los Fiery DFEs nunca almacenen las contraseñas de los usuarios localmente, lo que mejora significativamente la seguridad.

Medidas de seguridad de datos

Para proteger la información confidencial, los servidores de impresión Fiery implementan:

Almacenamiento cifrado: protege los trabajos de impresión y los datos de configuración

La encriptación de datos críticos del cliente garantiza que el almacenamiento seguro de las contraseñas y la información de configuración relacionada estén seguras en el Fiery DFE. Esta información crítica se cifra o se somete a un proceso de hash utilizando algoritmos criptográficos tales como AES-256 y SHA-2, que cumplen con los últimos estándares de seguridad.

Los datos del cliente almacenados en el disco seguirán siendo inaccesibles incluso en case de extraer el disco del Fiery DFE. La encriptación de datos del usuario puede habilitarse o deshabilitarse en Fiery DFEs basados en Windows. Para Fiery DFEs basados en Linux, la encriptación siempre está habilitada.

En el caso de que se olvide una frase de contraseña utilizada para la recuperación de datos, FIERY no podrá restablecerla, por lo que será necesario reinstalar el software por completo.

Los Fiery DFEs basados en Windows también ofrecen una opción para cifrar la unidad de arranque, que contiene el sistema operativo. Este cifrado ayuda a evitar ataques fuera de línea en el Fiery DFE y garantiza que la unidad de arranque no se pueda utilizar en otro dispositivo.

Borrado seguro: garantiza que los datos sean irrecuperables después de la eliminación

Los servidores de impresión de Fiery FS800 Pro basados en Windows son compatibles con el estándar de saneamiento de datos NIST 800-88. Los administradores de Fiery pueden configurar esta opción para los métodos de sobrescritura de imágenes de 1 pasada o de 3 pasadas.

Nota: La característica de borrado seguro no es compatible con las plataformas Fiery basadas en Linux y XB ni con los datos de usuario almacenados en unidades SSD.

Flujos de trabajo	Borrado seguro
Trabajos almacenados en la unidad de disco duro de Fiery DFE; borrado seguro configurado como **Encendido**	Sí
Trabajos almacenados en la unidad de disco duro de Fiery DFE; borrado seguro configurado como **Apagado**	No
Trabajos recibidos en Fiery DFE y eliminados tras configurar el borrado seguro como **Encendido**	Sí
Trabajos recibidos en Fiery DFE y eliminados antes de configurar el borrado seguro como **Encendido**	No

Flujos de trabajo	Borrado seguro
Copias del trabajo enviadas a otro Fiery DFE (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 DFE	No
Partes de un trabajo escritas en la unidad de disco duro de Fiery DFE 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 DFE desactivado antes de que se complete la eliminación del trabajo	No
Desfragmentación de la unidad de disco duro de Fiery DFE antes de eliminar un trabajo	No

Seguridad de red

Los Fiery DFEs emplean los siguientes mecanismos de seguridad para proteger las comunicaciones de red:

- Configuración de firewall, incluido el filtrado de IP y la administración de puertos
- Transport Layer Security (TLS) para comunicaciones cifradas (por ejemplo, HTTPS, LDAPS)
- IPSec para la comunicación segura cifrada de host a host
- SNMP v3 para herramientas seguras de supervisión y gestión de la red

Protocolos de red compatibles

FS800/FS800 Pro es compatible con una amplia gama de protocolos de red estándar del sector para garantizar la compatibilidad, la seguridad y la comunicación eficiente en diversos entornos. Por ejemplo:

- **Protocolos principales:** TCP/IP, IPv4, IPv6
- **Protocolos web:** HTTP/1.1, HTTPS (TLS 1.2/1.3)
- **Servicios de archivo e impresión:** FTP, LPR, IPP 2.0, SMB v2, SMB v3, Puerto 9100
- **Gestión y monitorización:** SNMP v1, v2c y v3
- **Acceso remoto:** RDP (solo servidores de impresión Fiery basados en Windows)
- **Seguridad y autenticación:** IPSec (IKEv2), LDAP v3, IEEE 802.1X
- **Servicios de red:** DHCP, DNS
- **Protocolos de detección:** WSD, Bonjour, SLP

Puertos de red

Por defecto, todos los puertos TCP/IP no utilizados están deshabilitados. El administrador de Fiery puede habilitar o deshabilitar los puertos de red según sea necesario. Al deshabilitar un puerto, se impide la conexión externa a través de ese puerto.

Puertos de entrada

Los Fiery DFEs supervisan y monitorizan las conexiones de red entrantes, permitiendo que solo el tráfico autorizado acceda al servidor y protegiéndolo contra accesos no autorizados o ataques.

TCP	UDP	Nombre del puerto	Servicios dependientes
20-21		FTP	FTP

TCP	UDP	Nombre del puerto	Servicios dependientes
80		HTTP	WebTools, IPP
135		MS RPC	Servicio RPC de Microsoft®. Se abrirá un puerto adicional en el rango 49152-65535 para ofrecer servicio de Apuntar e imprimir relacionado con SMB.
137-139		NETBIOS	Impresión en Windows Estos puertos se cierran por defecto debido a que NetBIOS no es seguro.
	161, 162	SNMP	Herramientas basadas en SNMP
	427	SLP	Protocolo de ubicación de servicios. Este puerto está bloqueado de forma predeterminada porque SLP no es seguro.
443		HTTPS	WebTools, IPPS
445		SMB/IP	SMB a través de TCP/IP
	500	ISAKMP	IPsec
515		LPD	Impresión LPR
631		IPP	IPP
3389		RDP	Escritorio remoto (solo Fiery DFEs basados en Windows)
3702	3702	WS-Discovery	Web Services for Devices (WSD) Permite la detección y la impresión en el Fiery DFE a través de WSD.
	4500	NAT transversal IPsec	IPsec
	5353	DNS de multidifusión (mDNS)	Bonjour
6310		DMP	Impresión móvil directa
8010		Puerto del Fiery	JDF
8021-8022		Puertos FIERY	Fiery Harmony, Fiery HotFolders y Fiery Command WorkStation
8090		Puerto del Fiery	OFA
9100-9103		Puertos de impresión	Puerto 9100
	9906	Puerto del Fiery	Discovery de Harmony
21030		Puerto del Fiery	Visualizador de imagen de Fiery

Nota: Los puertos IPSec (500 y 4500) solo se pueden configurar para los servidores FS800 (Fiery DFEs basados en Linux).

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 o deshabilitar los diferentes servicios dependientes que proporciona el Fiery DFE.

Puertos de salida

Los Fiery DFEs gestionan y restringen el tráfico de red saliente para garantizar que solo las comunicaciones autorizadas salgan del dispositivo, lo que reduce la exposición a amenazas externas.

Puertos de salida	Objetivo	Configuración predeterminada/Activada
53	DNS	Por defecto
67	DHCP	Por defecto
80, 443	Actualizaciones del Fiery System, actualizaciones de Windoes, JDF, PrintMe y otras comunicaciones en la nube	Por defecto
161, 162	SNMP	Configuración de IP dual
21	Explorar a FTP	En configuración
123	NTP	En configuración
389/636	Servicios LDAP	En configuración
445	Explorar a SMB/JobRegistrar a SMB/JDF Ruta global común	En configuración
500/4500	IPSEC	En configuración
8080/8443	HTTP/HTTPS/ Puerto de Proxy FTP	En configuración

Comunicación con los servicios en la nube

Esta lista enumera algunos servicios internos de Fiery y algunas aplicaciones que requieren comunicación con servicios externos basados en la nube; por ejemplo, para descargar actualizaciones de seguridad de Fiery o para la activación de licencias. Esta documentación resulta especialmente útil para los clientes que han deshabilitado todas las comunicaciones externas y están intentando hacer excepciones en su firewall corporativo.

Servicio/ Aplicación Fiery	Nombre de dominio totalmente cualificado/URL	Puerto	Ubicación del servidor	Información de uso
Actualización del sistema	https://liveupdate.fiery.com/des/hypatia.asmx	443	Fiery	Descargar actualizaciones de seguridad de Fiery
OFA	https://flexlicensing.fiery.com	443	Fiery	Activación de la licencia

Servicio/ Aplicación Fiery	Nombre de dominio totalmente cualificado/URL	Puerto	Ubicación del servidor	Información de uso
IQ	https://iq.fiery.com/iq	443	AWS	Nube Fiery IQ
LINQ	https://ews.fiery.com	443	Azure	Análisis
Impresión universal	Múltiples dominios: • portal.azure.com • print.print.microsoft.com • notification.print.microsoft.com • discovery.print.microsoft.com • graph.print.microsoft.com	80/443	Azure	Proxy IPP y servicio de impresión universal
SSO	login.microsoft.com	80/443	Microsoft	Inicio de sesión único
Servicios de actualización Windows Server (WSUS)	Múltiples dominios: • http://windowsupdate.microsoft.com • http://.windowsupdate.microsoft.com • https://.windowsupdate.microsoft.com • http://.update.microsoft.com • https://.update.microsoft.com • http://.windowsupdate.com • http://download.windowsupdate.com • https://download.microsoft.com • http://.download.windowsupdate.com • http://wustat.windows.com • http://ntservicepack.microsoft.com • http://go.microsoft.com • http://dl.delivery.mp.microsoft.com • https://dl.delivery.mp.microsoft.com • http://.delivery.mp.microsoft.com • https://.delivery.mp.microsoft.co	80/443	Microsoft	Actualizaciones de Windows

Servicio/ Aplicación Fiery	Nombre de dominio totalmente cualificado/URL	Puerto	Ubicación del servidor	Información de uso
Command WorkStation	Múltiples dominios: • https://help.fiery.com • https://learning.fiery.com • https://communities.fiery.com/s/ • https://liveupdate.fiery.com • https://iq.fiery.com	443	Fiery	Asistencia técnica de Fiery, actualizaciones del Fiery, Fiery Cloud

Filtrado de IP

El filtrado de IP permite al administrador controlar las peticiones de conexión al Fiery DFE basándose en direcciones IP predefinidas. Al definir las políticas por defecto, el administrador puede especificar si se deben permitir o denegar los paquetes de datos entrantes. Además, pueden crear filtros para un máximo de 16 direcciones IP o rangos, permitiendo o denegando las solicitudes de conexión en consecuencia.

Cada configuración de filtro IP especifica una dirección IP o un rango de direcciones IP y la acción correspondiente. Cuando la acción es Denegar, se descartan los paquetes con una dirección de origen que pertenezca a las direcciones especificadas. Por el contrario, cuando la acción es Aceptar, se permiten paquetes.

Autenticación de red

SNMP v3

El Fiery DFE es compatible con el estándar SNMPv3 más reciente, lo que facilita el uso de paquetes de comunicación cifrados para garantizar la confidencialidad, la integridad de los mensajes y la autenticación.

El administrador de Fiery puede elegir entre tres niveles de seguridad en SNMP: Mínimo, Medio o Máximo. En estos niveles, las contraseñas se cifran mediante algoritmos como SHA-1 o SHA-256, y se cifra todo el mensaje SNMP. Además, el administrador local puede configurar los nombres de comunidad de lectura y escritura SNMP junto con otros ajustes de seguridad.

IEEE 802.1x

802.1X es un estándar IEEE para el control del acceso a la red basado en puertos que garantiza que los dispositivos se autentiquen antes de acceder a la red local y sus recursos. En Fiery DFEs, 802.1X se puede configurar para utilizar EAP-MD5 Challenge o PEAP-MSCHAPv2 como métodos de autenticación basados en credenciales, o EAP-TLS para la autenticación basada en certificados. Fiery DFEs admiten solo certificados de usuario (no certificados de dispositivo) para la autenticación EAP-TLS. EAP-MD5 Challenge se proporciona por compatibilidad y es menos seguro que PEAP-MSCHAPv2 y EAP-TLS.

Fiery DFE realiza la autenticación 802.1X al inicio y cada vez que se restablece la conexión de red.

Encriptación de red

Seguridad del protocolo de Internet (IPsec)

IPsec mejora la seguridad de las comunicaciones basadas en IP mediante el cifrado y la autenticación de cada paquete en la capa de red, protegiendo así los datos en tránsito en todas las aplicaciones que utilizan IP. El Fiery DFE utiliza una autentificación de clave precompartida para establecer conexiones seguras con otros sistemas a través de IPsec. Una vez establecida la comunicación a través de IPsec entre un ordenador cliente y un Fiery DFE, todas las comunicaciones, incluidos los trabajos de impresión, se transmiten de forma segura a través de la red.

Hay protocolos, como LPR, puerto 9100, FTP, WSD y Harmony (protocolo propietario de Fiery), que se utilizan para el envío de trabajos de impresión, las actualizaciones del estado de los trabajos y los comandos administrativos. Estos protocolos no pasan por un canal seguro, por lo que las organizaciones que requieren protección de confidencialidad e integridad para tales funciones deben implementar IPsec entre el equipo cliente y el Fiery DFE.

HTTPS

Fiery DFEs Utiliza HTTPS a través de TLS para proteger las comunicaciones basadas en web y API entre los clientes y los componentes del servidor. Fiery DFEs es compatible con TLS 1.3 y TLS 1.2, lo que proporciona una sólida protección criptográfica y características de seguridad modernas. HTTPS es obligatorio para las conexiones a WebTools y Fiery API, lo que garantiza que el tráfico administrativo y operativo transportado a través de estas interfaces esté cifrado en tránsito y protegido contra interceptaciones o manipulaciones. No toda la comunicación cliente-servidor se realiza a través de HTTPS.

Gestión de certificados

Fiery DFEs ofrece una interfaz para administrar los certificados utilizados durante las comunicaciones TLS. Fiery DFEs admite certificados X.509 en formato PEM, codificados en Base64, utilizando claves RSA con longitudes de 4096, 3072 o 2048 bits.

La gestión de certificados permite al administrador de Fiery realizar las siguientes acciones:

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

Los certificados digitales autofirmados proporcionan cifrado, pero no ofrecen validación automática de confianza. Para una distribución segura, se recomienda utilizar certificados emitidos por una entidad de certificación (CA) de confianza para garantizar una verificación de identidad adecuada.

Una vez que el certificado haya sido firmado por una CA de confianza, se puede cargar en el Fiery DFEen la sección Configure de WebTools.

Server Message Block (SMB)

SMBv1, el protocolo antiguo para compartir archivos e impresoras, está deshabilitado en los Fiery DFEs debido a vulnerabilidades de seguridad conocidas. En su lugar, Fiery DFEs es compatible con SMBv2 y SMBv3. La firma SMB se aplica, lo que garantiza que todos los paquetes estén firmados digitalmente para evitar ataques de intermediario. Cuando se habilita la autenticación SMB, los usuarios deben proporcionar un nombre de usuario y una contraseña

válidos para acceder a las carpetas y el contenido compartidos. La impresión o el uso compartido de archivos a través de SMB para una cuenta de invitado también puede restringirse estableciendo una contraseña en Fiery Configure.

Seguridad del hardware

Los Fiery DFEs se han diseñado pensando en seguridad del hardware de calidad empresarial. La protección de la información confidencial no se limita a los controles de software. Los componentes de hardware desempeñan un papel fundamental a la hora de mantener la integridad del sistema y la confidencialidad de los datos. A continuación se describen los elementos clave del hardware y sus medidas de seguridad.

Memoria volátil (RAM)

Los Fiery DFEsutilizan memoria volátil (RAM) para almacenar temporalmente datos durante las operaciones activas. Para mitigar el riesgo de exposición de datos:

- La información confidencial de la RAM se borra inmediatamente después de su uso o tras apagar el sistema.
- Las técnicas de depuración de memoria se aplican para evitar que los datos residuales persistan.
- El acceso a la RAM está restringido debido a la separación de privilegios impuesta por el procesador y el sistema operativo.

Memoria no volátil y almacenamiento de datos

La memoria no volátil, incluidos los discos duros, las unidades de estado sólido (SSD) y otros almacenamientos persistentes, conserva los datos incluso cuando el sistema está apagado. Las medidas de seguridad incluyen:

- Cifrado de datos del usuario (UDE) para proteger los datos almacenados.
- Métodos de eliminación segura para reproducción la información confidencial irrecuperable cuando se eliminan los archivos.

Memoria Flash

La memoria flash se utiliza para almacenar el firmware, los archivos de configuración y la configuración del sistema. Para mantener su seguridad:

- El firmware está firmado digitalmente para evitar manipulaciones.
- Las actualizaciones de firmware se verifican mediante sumas de comprobación criptográficas antes de la instalación.
- Los mecanismos de protección contra escritura evitan modificaciones no autorizadas durante el tiempo de ejecución.

CMOS y NVRAM

Los parámetros críticos del sistema, como las configuraciones de hardware y los valores de arranque, se almacenan en CMOS y RAM no volátil (NVRAM). Para proteger estos datos:

- El acceso está restringido a los procesos administrativos autorizados.
- Secure Boot ayuda a garantizar que solo se carguen firmware y componentes de arranque de confianza.
- Las variables NVRAM críticas están protegidas contra daños y modificaciones no autorizadas mediante controles de integridad.

Unidades de almacenamiento

Fiery DFEs utiliza unidades de almacenamiento para el sistema operativo host, archivos del sistema, almacenamiento en cola de trabajos, registros y archivos temporales.

Se proporcionan las siguientes características de seguridad para proteger los datos del cliente:

- Cifrado a nivel de unidad.
- Listas de control de acceso (ACL) para restringir las operaciones de lectura/escritura no autorizadas.
- Los kits de seguridad para unidades de disco (opcionales para los Fiery DFEs externos) permiten bloquear las unidades de forma segura durante su funcionamiento normal.

Puertos físicos

Los puertos físicos, como USB, interfaces de red y conectores de servicio, son vectores potenciales para el acceso no autorizado. La seguridad del hardware de Fiery aborda este riesgo de la siguiente manera:

- Deshabilitar los puertos no utilizados mediante controles de hardware y firmware.
- Restricción del acceso de dispositivos externos mediante controles administrativos y configuración del sistema.
- Registro de eventos relevantes para la seguridad que implican interfaces físicas críticas.

Al integrar estas medidas de seguridad de hardware con el software y las protecciones de red, los Fiery DFEsofrecen una estrategia integral de defensa en profundidad, que garantiza la confidencialidad, integridad y disponibilidad de los datos confidenciales en los entornos de impresión.

Integridad del sistema y actualizaciones seguras

Mantener la integridad del sistema es primordial para garantizar la seguridad. Fiery DFEs proporciona la siguiente asistencia:

- Registros de auditoría de seguridad
- Arranque seguro: garantiza que solo se cargue software de confianza.
- Actualizaciones firmadas digitalmente: evita la manipulación de las actualizaciones de software.
- Gestión automatizada de actualizaciones de seguridad: simplifica el proceso de aplicación de actualizaciones de seguridad.

Registro de auditoría de seguridad

Los administradores con privilegios elevados pueden acceder y examinar los eventos de seguridad registrados en el Registro de auditoría de seguridad. Este registro está habilitado por defecto.

Cada evento de seguridad está categorizado como Información, Advertencia o Error. El administrador no recibe alertas ni notificaciones; En su lugar, se les presenta un registro estático.

Los registros están formateados para ser compatibles con las herramientas de administración de eventos e información de seguridad (SIEM) que se utilizan habitualmente para la recopilación y el análisis de registros. Todos los datos de eventos capturados cumplen con los estándares descritos en NIST SP 800-53.

El administrador de Fiery puede acceder al registro de auditoría de seguridad sin necesidad de la intervención de FIERY. Los registros de los servidores de impresión Fiery basados en Linux se proporcionan en formato Syslog (RFC 5424 o RFC 3164). En el caso de los servidores de impresión Fiery basados en Windows, los registros se guardan en el formato EVTX estándar de Windows y se pueden leer desde el Administrador de registros de eventos de Windows y muchas soluciones comerciales disponibles que usan la API de registro de eventos de Windows. Los servidores de impresión Fiery basados en Linux ofrecen la posibilidad de reenviar registros a un sistema de recopilación centralizado como Syslog.

Los registros de seguridad se conservan según la capacidad de almacenamiento en disco local, hasta un límite preestablecido En Fiery DFEs basados en Windows, los eventos individuales más antiguos se eliminan según sea necesario. En Fiery DFEs basados en Linux, los registros de auditoría se rotan según el tamaño del archivo; los archivos de registro girados se conservan hasta el número de rotaciones configurado, después de lo cual se eliminan los archivos girados más antiguos.

Secure Boot

Secure Boot protege el sistema operativo durante el inicio al permitir que solo se carguen componentes de confianza firmados digitalmente. En los servidores de impresión de Fiery basados en Windows, evita que se ejecute código no autorizado o malintencionado en el arranque, lo que reduce el riesgo de que se vea comprometido. Para que la función Secure Boot sea efectiva, debe estar habilitada en la configuración de la BIOS y debe estar activada.

Actualizaciones firmadas digitalmente

Los Fiery DFEs utilizan actualizaciones firmadas digitalmente para garantizar la integridad y autenticidad de todas las instalaciones de software y firmware. Cada actualización está firmada criptográficamente por Fiery o sus socios autorizados, lo que permite al servidor de impresión verificar que el contenido no ha sido alterado ni manipulado. Este proceso protege contra la introducción de código malicioso y garantiza que solo se apliquen actualizaciones confiables, manteniendo la seguridad y confiabilidad del sistema.

Gestión automatizada de actualizaciones de seguridad

Las actualizaciones oportunas de software son vitales para un funcionamiento óptimo de Fiery DFEs. La instalación de las actualizaciones de seguridad son importantes para mantener la seguridad de los Fiery DFEs en un entorno de impresión determinado.

La **actualización del sistema Fiery** descarga e instala las actualizaciones de seguridad si la opción está habilitada en el Fiery DFE. Por defecto, esta opción está habilitada y se recomienda dejarla activada.

Las vulnerabilidades de seguridad del sistema operativo Microsoft® Windows™ no se detallan en este documento, ya que Microsoft las maneja directamente y las distribuye a los clientes a través de **actualizaciones de Windows** cuando están disponibles.

Para abordar las inquietudes acerca de la seguridad y las vulnerabilidades que podrían afectar a los componentes básicos del hardware Fiery, incluidos la placa base, el procesador y el firmware, FIERY colabora estrechamente con los fabricantes para obtener las actualizaciones de seguridad necesarias. Estas actualizaciones de seguridad se proporcionan posteriormente a los clientes según sea necesario.

Nota: Las actualizaciones de software Fiery están firmadas digitalmente mediante Secure Hash Algorithm (SHA-2) para evitar modificaciones no autorizadas, incluida la inserción de malware.

Actualizaciones de seguridad del software Fiery DFE

Las actualizaciones oportunas del software son fundamentales para el funcionamiento óptimo del Fiery DFE. Al aplicar las últimas actualizaciones de seguridad del software del Fiery DFE, se garantiza la integridad del sistema, se mitigan las vulnerabilidades y se mantiene el cumplimiento de los estándares de seguridad del sector.

El equipo de seguridad del Fiery DFE supervisa y realiza un seguimiento diligente de las vulnerabilidades de seguridad a través de una amplia red de fuentes fiables y de confianza, como:

- Alertas y avisos de la Agencia de Seguridad de Infraestructura y Ciberseguridad de EE. UU. (CISA)
- Base de datos de vulnerabilidad nacional del Instituto Nacional de Estándares y Tecnología (NIST) de EE. UU.
- Registros de vulnerabilidades y exposiciones comunes (CVE)
- Informes y avisos del Centro de Coordinación del CERT (CERT/CC) sobre vulnerabilidades de software y hardware
- Gobierno Regional y Agencias Reguladoras
- Avisos de seguridad de proveedores de software y hardware

Fiery da prioridad a las correcciones de seguridad en función de la gravedad (crítica, alta, media y baja) determinada por el sistema común de puntuación de vulnerabilidades (CVSS). Estas correcciones se publican después de obtener la aprobación correspondiente del colaborador fabricante de equipos originales (OEM). Una vez aprobadas, las actualizaciones de seguridad del software Fiery pasan a estar disponibles para la descarga. Todas las actualizaciones de software Fiery están firmadas digitalmente mediante Secure Hash Algorithm (SHA-2) para evitar modificaciones no autorizadas, incluida la inserción de malware.

Cuando está activada, la actualización del sistema Fiery descarga e instala automáticamente las actualizaciones de seguridad en el Fiery DFE. Por defecto, esta opción está habilitada y se recomienda encarecidamente que los clientes mantengan su estado activo.

Cumplimiento y mejores prácticas

Las implementaciones de seguridad sólidas se ajustan a los estándares fundamentales de la industria y los marcos regulatorios, que incluyen:

- RGPD, Ley de Datos de la UE
- FIPS 140-3
- NIST 800-88. Guías generales para la desinfección del papel (solo FS800 Pro)
- NIST 800-52. Directrices para la selección, configuración y uso de implementaciones de seguridad de la capa de transporte (TLS)
- Certificación del Modelo de Madurez de Ciberseguridad (CMMC) del Departamento de Defensa de EE. UU. Nivel 2: Protección amplia de la información no clasificada controlada (CUI) (solo FS800 Pro)
- NIST 800-193. Directrices de resistencia del firmware de la plataforma (solo FS800 Pro)
- NIST 800-53. Controles de seguridad y privacidad para sistemas de información y organizaciones
- Perfil de protección de criterios comunes para sistemas operativos de uso general (solo FS800 Pro)

Para reforzar la postura de seguridad, los administradores de TI son responsables de implementar las siguientes medidas:

- Aplicación periódica de actualizaciones de seguridad
- Aplicación de políticas de autenticación sólidas
- Realización de auditorías de seguridad periódicas
- Implementación de la segmentación de red para entornos de impresión

Indicaciones generales para la configuración segura del Fiery DFE

Los administradores de Fiery pueden seguir estas indicaciones generales para reforzar la seguridad al configurar el Fiery DFE.

Cambiar la contraseña del administrador

Fiery DFEs vienen de fábrica con una contraseña por defecto para la cuenta de administrador. Esta contraseña concede acceso completo al Fiery DFE, tanto de forma local como desde un cliente remoto. Este acceso abarca, pero no se limita a:

- Sistema de archivos (solo Fiery DFEs en Windows)
- Configuración del sistema de seguridad
- Configuración de aplicaciones
- Entradas del registro

Se recomienda encarecidamente cambiar la contraseña de administrador Fiery por defecto inmediatamente después de su instalación y de manera periódica según las políticas de seguridad de su organización. La contraseña de administrador de Fiery debe modificarse en la plataforma Fiery.

Prácticas recomendadas de funcionamiento seguro y eficiente

- Restrinja SNMP a la versión 3 para obtener la máxima seguridad.
- Deshabilite WSD para el envío de trabajos a fin de impedir su uso en los flujos de trabajo de impresión.
- Deshabilite los protocolos de impresión de Windows (LPR, puerto 9100, IPP) a menos que sea necesario.
- Habilite el filtrado de puertos TCP/IP para bloquear los puertos no utilizados y reducir el riesgo.
- Cierre los puertos 137–139 y 445 si no son necesarios para la impresión o el uso compartido de archivos en Windows.
- Desactive HTTP en el puerto 80 para evitar comunicaciones no seguras.
- Habilite la impresión segura para que solo el propietario del trabajo pueda enviar los trabajos de impresión.

Entornos de alta seguridad

Los administradores con privilegios elevados pueden configurar sin esfuerzo las opciones de alta seguridad seleccionando el perfil de alta seguridad disponible en **Configurar** > **Seguridad** de **WebTools**.

Conclusión

Los Fiery DFEs, aunque están equipados con sólidas características de seguridad, no están diseñados para estar conectados a Internet. Deben distribuirse en un entorno de red seguro con el acceso cuidadosamente controlado por el administrador de red. Diseñados para cumplir los estándares más recientes del sector, los Fiery DFEs, ofrecen seguridad de calidad empresarial para proteger los entornos de impresión frente a las amenazas cibernéticas en constante evolución. Los administradores pueden garantizar el cumplimiento y salvaguardar los datos confidenciales aprovechando al máximo las funciones de seguridad de Fiery.

Novedades de FS800, FS800 Pro

- Módulos del sistema principal actualizados para abordar las vulnerabilidades de seguridad.
- Las conexiones de escritorio remoto con Windows 11 son compatibles con Fiery DFEs TLS 1.3, lo que proporciona un cifrado mejorado y una seguridad de conexión mejorada.