FreeFlow Core, Versione 4.0
agosto 2014
708P90733

Xerox® FreeFlow® Core

Guida alla protezione

Versione documento 1.0, agosto 2014

BR10173

Indice generale

Indice generale

1

Protezione delle applicazioni FreeFlow Xerox®

Descrizione

Nel presente documento vengono fornite informazioni relative alla protezione di FreeFlow Core.

In Xerox, i problemi di protezione sono tenuti in massima considerazione. In qualità di leader nello sviluppo di tecnologie digitali, Xerox ha dimostrato il massimo impegno nel mantenere le informazioni digitali sicure e protette identificando possibili vulnerabilità e attivandosi per limitare i rischi. Xerox si impegna a offrire il prodotto software più sicuro possibile in base alle informazioni e tecnologie disponibili, preservando prestazioni, valore, funzionalità e produttività. I componenti di FreeFlow vengono controllati per garantire la conformità agli standard di sicurezza utilizzando gli strumenti di scansione disponibili in commercio. I vari punti di vulnerabilità delle applicazioni vengono individuati in base ai risultati raggiunti mediante indagini interne.

Abilitazione e configurazione del firewall

Si consiglia di abilitare un firewall sul server FreeFlow Core. È necessario che le porte siano bloccate a meno che debbano eseguire una determinata funzione come illustrato di seguito:

Porta	Protocollo o applicazione	Funzione FreeFlow Core abilitata
80	HTTP	In entrata – Avvio dell'interfaccia utente FreeFlow Core In uscita – Recupero di file elencati in Manifest o nelle preselezioni Componenti
161,162	SNMP	In uscita – Identificazione del tipo di DFE durante l'impostazione della stampante
631	IPP	In uscita – Invio di lavori ai DFE
25, 2525, 465, 475, 587	SMTP	In uscita – Invio di notifiche e-mail Nota: il numero di porta richiesto dipende dalla configurazione del server SMTP
TCP, UDP: 7751	JMF	In entrata – Ricezione di richieste JMF/JDF
Varie	JMF	In uscita – Restituzione di segnali di stato JMF. Il client JMF specifica il numero di porta.
139, 445	SMB	In entrata – Condivisione di cartelle attive tramite la condivisione file di Windows In uscita – Utilizzo di cartelle attive in directory condivise In uscita – Recupero di file elencati in Manifest da directory condivise In uscita – Recupero di file elencati in Componenti da directory condivise In uscita – Salvataggio in directory condivise
20,21	FTP	In entrata – Condivisione di cartelle attive tramite FTP In uscita – Recupero di file elencati in Manifest o nelle preselezioni Componenti
443	HTTPS	In entrata – Condivisione di file per il sistema FreeFlow Core remoto In uscita – Recupero di file dal sistema FreeFlow Core remoto

Regole Windows Firewall

1. Passare a **Pannello di controllo > Sistema e sicurezza > Windows Firewall > Impostazioni avanzate**.
2. Per ciascuna regola richiesta, selezionare **Regole in entrata** o **Regole in uscita**:
   a) In Azioni, fare clic su **Nuova regola**. Viene visualizzata Creazione guidata nuova regola connessioni in entrata.
   b) Fare clic su **Porta** per il tipo di regola. Selezionare **Avanti**.
   c) Fare clic su **TCP** o **UDP** come riportato nella tabella qui sopra. Immettere un valore in Porte locali specifiche come riportato nella tabella qui sopra. Selezionare **Avanti**.
   d) Fare clic su **Consenti la connessione**. Selezionare **Avanti**.
   e) Selezionare tutte le caselle. Selezionare **Avanti**.

Protezione da virus

Xerox adotta speciali precauzioni per garantire che il software venga fornito senza contaminazioni di virus informatici. Si raccomanda tuttavia di dotarsi di uno dei software di rilevamento virus più diffusi nel settore. Per proteggere il sistema da virus, è necessario che il software di rilevamento virus sia costantemente aggiornato.

Per migliorare le prestazioni si consiglia di escludere le directory di installazione di FreeFlow Core e MS SQL Server dalla scansione antivirus.

In alternativa, è possibile escludere dalla scansione antivirus le seguenti cartelle di FreeFlow Core:

- <FreeFlow Core Installation directory>\Platform\Spool
- <FreeFlow Core Installation directory>\Logs
- <FreeFlow Core Installation directory>\Platform\Logs
- <FreeFlow Core Installation directory>\Web\Logs
- <FreeFlow Core Installation directory>\Config
- <FreeFlow Core Installation directory>\Presets

Aggiornamento del software

Si consiglia di aggiornare costantemente tutti i prodotti installati sul server FreeFlow Core. Microsoft Update andrebbe eseguito almeno una volta al mese.

I Service Pack del sistema operativo non devono essere installati tramite Microsoft Update fino a quando non si riceve una comunicazione formale dal servizio di assistenza.

Xerox distribuisce bollettini di avviso mensili, se richiesto, in cui vengono elencati gli aggiornamenti che devono essere "esclusi" sul sistema FreeFlow. Queste informazioni vengono anche pubblicate sul sito Web www.xerox.com/security nella sezione relativa alle istruzioni sulla sicurezza dei prodotti. Gli aggiornamenti ad alta priorità e legati alla protezione sono critici e devono sempre essere installati a meno che non vengano specificatamente esclusi.