Versione 5.4.0
Novembre 2019
702P07033

Xerox® FreeFlow® Core

Guida alla sicurezza di

©2019 Xerox Corporation. Tutti i diritti riservati. Xerox®, Xerox con il marchio figurativo® e FreeFlow® sono marchi di Xerox Corporation negli Stati Uniti e/o in altri paesi.

Questo software include software sviluppato da Adobe Systems Incorporated.

Adobe, il logo Adobe, il logo Adobe PDF, PDF Converter SDK, Adobe Acrobat Pro DC, Adobe Reader DC e PDF Library sono marchi o marchi registrati di Adobe Systems Incorporated negli Stati Uniti e/o in altri paesi.

Il browser Google Chrome™ è un marchio di Google LLC.

Microsoft®, Windows®, Edge®, Microsoft Language Pack, Microsoft Office 2013, Microsoft Office 2016, Microsoft SQL Server e Internet Explorer® sono marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Apple®, Macintosh®, Mac®, Mac OS® e Safari® sono marchi o marchi registrati di Apple, Inc. negli Stati Uniti e in altri paesi.

Mozilla Firefox è un marchio di Mozilla Foundation negli Stati Uniti e in altri paesi.

BR14707

Sommario

1

Panoramica

Questo capitolo contiene:

Finalità

Lo scopo di questo documento è fornire informazioni su Xerox® FreeFlow® Core e Xerox® FreeFlow® Cloud in materia di sicurezza del prodotto.

Il cliente è responsabile della sicurezza della propria rete e del prodotto FreeFlow. Il prodotto FreeFlow non applica norme di sicurezza per alcun ambiente di rete.

Destinatari

Questo documento è progettato per i clienti che richiedono maggiori informazioni sulla sicurezza relative a Xerox® FreeFlow® Core.

Declinazione di responsabilità

Le informazioni contenute in questo documento sono accurate alla data della sua pubblicazione. Dette informazioni vengono fornite senza alcuna garanzia. In nessuna circostanza Xerox® Corporation sarà ritenuta responsabile per danni risultanti dall'utilizzo o mancato utilizzo delle informazioni fornite in questo documento, ivi inclusi danni diretti, indiretti, incidentali, consequenziali, causanti perdita di profitto o speciali, anche qualora Xerox® Corporation sia stata messa al corrente della possibilità di tali danni.

2

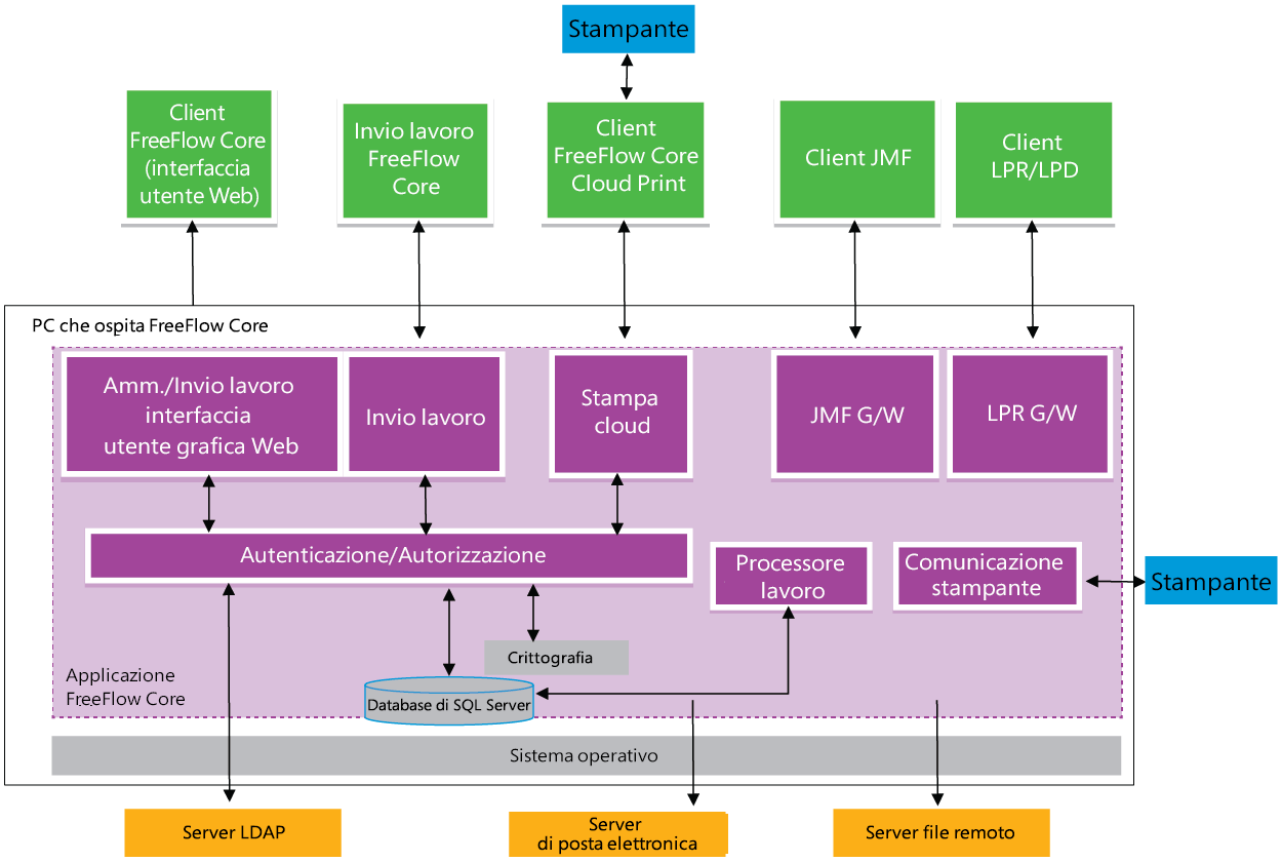
Descrizione del prodotto

Questo capitolo contiene:

Xerox® FreeFlow® Core è lo stato dell'arte nel campo delle soluzioni di flusso di lavoro di Xerox. FreeFlow Core è una soluzione basata su browser che automatizza e integra l'elaborazione dei lavori di stampa, dalla preparazione dei file alla produzione finale. Con FreeFlow Core si ottiene un flusso di lavoro senza operazioni manuali che funziona in modo semplice, si adatta facilmente, è scalabile con rapidità e fornisce risultati costanti.

Xerox® FreeFlow® Core Cloud è l'offerta della soluzione con configurazione basata su cloud. Esecuzione su cloud significa che Xerox installerà il software sui propri server cloud. Xerox si occupa di configurare e gestire la manutenzione del prodotto. L'utente può accedere al proprio dispositivo dedicato e protetto da un browser web.

Struttura del software di sistema



3

Aspetti legati alla sicurezza di alcune funzioni

Questo capitolo contiene:

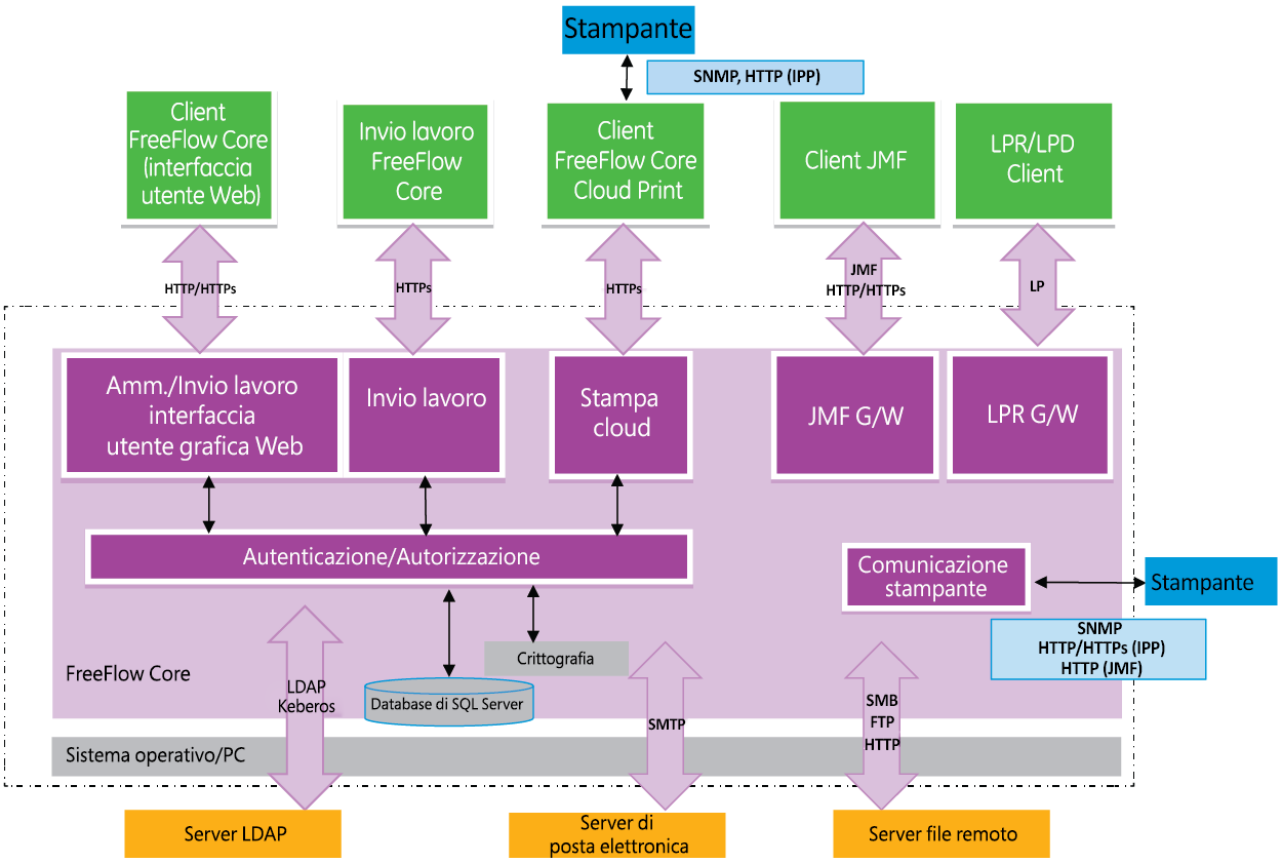
Accesso al sistema

Connessioni di rete

Per Xerox® FreeFlow® Core è richiesta una connessione di rete sia per l'elaborazione dei lavori che per le interazioni degli utenti. Consultare le informazioni sulla sicurezza di ogni connessione di rete.

Nota: Per fornire maggiore protezione contro eventuali attacchi informatici, abilitare Windows Firewall sul server su cui è installato FreeFlow Core.

FreeFlow Core utilizza le seguenti connessioni del protocollo di rete.



Client Xerox® FreeFlow® Core

La connessione a FreeFlow Core richiede un browser Web compatibile con HTML5 e CSS3. Sono richieste connessioni HTTPS per fornire un download sicuro del client Xerox® FreeFlow® Core, nonché una comunicazione protetta tra il client e Xerox® FreeFlow® Core.

- Per abilitare le connessioni HTTPS, aggiungere un certificato TLS/SSL a ISS (Internet Information Services). Seguire le indicazioni disponibili nella documentazione Windows.
- Per abilitare le connessioni HTTPS, aggiungere un certificato CA alla gestione ISS (Internet Information Services). Fare riferimento alla documentazione Windows.
- FreeFlow Core supporta i protocolli di crittografia TLS 1.1 e 1.2. TLS 1.0. Tutte le versioni di SSL sono disabilitate.
- Se non vengono scaricati dei file di lavoro, nessun dato del cliente viene scambiato tra il client e il server Xerox® FreeFlow® Core.

Nota: Il client recupera le proprietà del lavoro che contengono i dati del cliente.

Tabella 3.1 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
80	HTTP	In entrata **Nota:** Il numero di porta dipende dalla configurazione del server IIS.
443	HTTPS	In entrata **Nota:** Il numero di porta dipende dalla configurazione del server IIS.

Ruoli utente

Per impostazione predefinita, Xerox® FreeFlow® Core si apre visualizzando una schermata di accesso.

- Per accedere al dispositivo FreeFlow Core, gli utenti devono eseguire il login.
- Gli utenti connessi vengono automaticamente disconnessi dopo 30 minuti di inattività.
- Se l'autenticazione di FreeFlow Core ha esito negativo, gli utenti non vengono bloccati.

Per assegnare i ruoli agli utenti, consultare la sezione *Impostazione dell'accesso utente* della Guida di FreeFlow Core.

Ruolo Amministratore

Gli amministratori hanno accesso all'intero sistema:

- Funzioni della scheda Stato e Gestione lavori: Schede Invia lavoro e Stato lavoro.
- Schede Stato e Gestione stampante
- Impostazione flusso di lavoro
- Funzioni della scheda Amministratore:
  - Impostazione cartella attiva
  - Impostazione delle notifiche
  - Impostazione accesso utente
- Utilità di Core Server disponibili sul desktop del server:
  - Xerox® FreeFlow® Core Exchange
  - Rapporti Xerox® FreeFlow® Core
  - Xerox® FreeFlow® Core Cloud Print Server
  - Certificati Xerox® FreeFlow® Core
  - Licenza Xerox® FreeFlow® Core
  - Configurazione Xerox® Core
- Utilità del client Core:

  - Invio lavoro Xerox® FreeFlow® Core
  - Client Xerox® FreeFlow® Core Cloud Print

Nota: Un solo amministratore alla volta può essere connesso a Xerox® FreeFlow® Core.

Ruolo Operatore

Gli operatori hanno accesso a:

- Funzioni della scheda Stato e Gestione lavori: Schede Invia lavoro e Stato lavoro
- Schede Stato e Gestione stampante
- Utilità del client Core:
  - Invio lavoro Xerox® FreeFlow® Core
  - Client Xerox® FreeFlow® Core Cloud Print

Nota: Più operatori possono essere connessi contemporaneamente a Xerox® FreeFlow® Core.

Ruolo Supervisore stato lavoro

Il Supervisore stato lavoro ha accesso in sola lettura alla scheda Stato lavoro.

Nota: Più utenti, a cui è stato assegnato il ruolo Supervisore stato lavoro, possono essere connessi contemporaneamente a Xerox® FreeFlow® Core.

Autenticazione utente

Le credenziali immesse nel client del browser di Xerox® FreeFlow® Core sono crittografate con AES128. Le credenziali vengono crittografate prima essere inviate al server Xerox® FreeFlow® Core.

- Se si esegue l'autenticazione tramite Xerox® FreeFlow® Core, le informazioni degli utenti sono crittografate con AES128. Le credenziali sono archiviate localmente.
- Se si esegue l'autenticazione tramite Active Directory, le credenziali vengono decrittografate prima di essere inviate ad Active Directory. Quando si esegue l'autenticazione tramite Active Directory, le credenziali non vengono archiviate localmente.

La connessione della configurazione di Xerox® FreeFlow® Core ad Active Directory viene crittografata in base alla configurazione del sistema operativo.

Tabella 3.2 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
80	HTTP	In entrata **Nota:** Il numero di porta dipende dalla configurazione del server IIS.
88	Kerberos	In uscita: Autenticazione utente **Nota:** I numeri di porta e i servizi dipendono dalla configurazione di Active Directory sul server.
• 389 • 636 • 3268 • 3269	• LDAP • LDAP SSL • LDAP GC • LDAP GC SSL	In uscita: Convalida i gruppi AD durante la configurazione dell'autenticazione AD **Nota:** I numeri di porta e i servizi dipendono dalla configurazione di Active Directory sul server.

Connessione a SQL Server

Xerox® FreeFlow® Core comunica con SQL Server tramite Microsoft® Entity Framework. La comunicazione crittografata tra Xerox® FreeFlow® Core e SQL Server viene abilitata quando SQL Server è configurato per utilizzare le connessioni crittografate.

Le credenziali crittografate di SQL Server vengono archiviate localmente nel server Xerox® FreeFlow® Core.

Per eseguire l'installazione del software su un SQL Server remoto senza disporre di privilegi amministrativi SQLS, creare due database vuoti nell'istanza SQLS:

- `OapMasterDatabase`
- `OapPlatformDatabase`

Porta	Protocollo o applicazione	Tipo di connessione del firewall
1433	SQLS	In entrata: Riceve connessioni da Xerox® FreeFlow® Core In uscita: Comunica con il motore di stampa di database di SQL Server **Nota:** Il numero di porta dipende dalla configurazione del server SQLS.
1434	Servizio SQLS Browser	In entrata: Riceve connessioni da Xerox® FreeFlow® Core In uscita: Comunica con il motore di stampa di database di SQL Server **Nota:** Il server fornisce al client il numero di porta per la connessione.

Interfaccia utente Invia lavoro

L'interfaccia utente Invia lavoro utilizza la connessione del client Xerox® FreeFlow® Core per l'inoltro dei lavori. Per ulteriori informazioni, fare riferimento a Client Xerox® FreeFlow® Core.

Tabella 3.3 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
80	HTTP	In entrata **Nota:** Il numero di porta dipende dalla configurazione del server IIS.
443	HTTPS	In entrata **Nota:** Il numero di porta dipende dalla configurazione del server IIS.

Cartelle attive

Utilizzare le condivisioni file usate per condividere una cartella attiva locale e per accedere a Cartella attiva nelle cartelle Windows condivise. Per crittografare le cartelle Windows, utilizzare il file system Windows. Per proteggere le cartelle Windows, utilizzare il controllo accessi degli account utente di Windows.

Nota: Quando si utilizza il controllo accessi degli account utente, utilizzare lo stesso account di servizio usato per la configurazione delle *Procedure di installazione opzionali*. Per ulteriori informazioni, consultare la *Guida all'installazione di FreeFlow Core*.

Tabella 3.4 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
139, 445	SMB	In entrata: Condivide le cartelle attive tramite la condivisione file di Windows In uscita: Utilizza le cartelle attive in directory condivise
20, 21	FTP	In entrata: Condivide le cartelle attive tramite FTP

Elaborazione Manifest

Durante l'invio di manifest, Xerox® FreeFlow® Core recupera i file elencati nel manifest, a cui si può fare riferimento utilizzando unità mappate o percorsi di file UNC, URI HTTP o URI FTP.

Nota: Gli URI HTTP e FTP non supportano la crittografia.

Utilizzare le condivisioni file usate per condividere una cartella attiva locale e per accedere a Cartella attiva nelle cartelle Windows condivise. Per crittografare le cartelle Windows, utilizzare il file system Windows. Per proteggere le cartelle Windows, utilizzare il controllo accessi degli account utente di Windows.

Nota: Quando si utilizza il controllo accessi degli account utente, utilizzare lo stesso account di servizio usato per la configurazione delle procedure di installazione opzionali. Per ulteriori informazioni, vedere la sezione *Procedure di installazione opzionali* nella *Guida all'installazione di FreeFlow Core*.

Tabella 3.5 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
139, 145	SMB	In uscita: Recupera i file elencati in Manifest da directory condivise
20, 21	FTP	In uscita: Recupera i file elencati in Manifest
80	HTTP	In uscita: Recupera i file elencati in Manifest

LPD (Line Printer Daemon)

Nota: I comandi LP (Line Printer) non supportano le connessioni protette.

Tabella 3.6 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
515	LP	In entrata: Riceve richieste LPR (Line Printer Remote) e comandi LP

Segnali di stato stampante e comandi JMF

I comandi JMF (Job Messaging Format) supportano le connessioni protette. Il recupero dei file JMF utilizza connessioni non crittografate.

Nota: L'invio JMF protetto richiede l'invio di un pacchetto MIME con i file JMF, JDF e PDF.

Per i segnali di stato della stampante JMF viene utilizzata una connessione non crittografata. Per ricevere un avviso di stato della stampante JMF in modalità protetta, inviare il comando StatusQuery di JMF tramite una connessione protetta.

Per abilitare la comunicazione HTTPS per i comandi JMF:

1. Per aggiungere un certificato all'archivio chiavi di Java, usare l'utilità **installJMFCertificate.bat** contenuta nella directory di installazione di Xerox® FreeFlow® Core.
2. Riavviare il servizio del server JMF di Xerox® FreeFlow® Core.
3. Per testare l'installazione, accedere a `http://<hostname>:7759`. Se JMF protetta è configurata correttamente, nel browser viene visualizzata la pagina di errore `HTTP Status 404`.

Tabella 3.7 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
7751	JMF	In entrata: Riceve i comandi JMF
Varia	JMF	In uscita: Restituisce i segnali di stato della stampante JMF **Nota:** Il numero di porta richiesto viene definito dal client che richiede i segnali di stato stampante JMF o la restituzione del segnale di stato JMF.
7759	sJMF	In entrata: Riceve i comandi JMF protetti

Invio lavoro Xerox® FreeFlow® Core

La connessione tra Invio lavoro Xerox® FreeFlow® Core e Xerox® FreeFlow® Core è sempre crittografata e richiede l'installazione di un certificato CA.

- Per installare il certificato nel server, aggiungere il certificato usando Gestione Internet Information Services (IIS).
- Tra Invio lavoro Xerox FreeFlow Core e il software Xerox FreeFlow Core si utilizza TLS 1.2.
- Sia l'applicazione Invio lavoro Xerox® FreeFlow® Core che i componenti aggiuntivi di Microsoft Office utilizzano la stessa connessione protetta a Xerox® FreeFlow® Core.
- Le credenziali crittografate vengono archiviate localmente.

Tabella 3.8 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
443	HTTPS	In ingresso nel server: Accetta le connessioni dal client di Invio lavoro Xerox® FreeFlow® Core In uscita nel client: Invia lavori di Xerox® FreeFlow® Core Cloud

Nodi del flusso di lavoro

I componenti del flusso di lavoro che recuperano o salvano i file di lavoro potrebbero usare unità mappate, percorsi di file UNC, URI HTTP o FTP.

Nota: Gli URI HTTP e FTP non supportano la crittografia.

Per crittografare le condivisioni file utilizzate per la condivisione, utilizzare il file system Windows. Per proteggere le condivisioni file, utilizzare il controllo accessi degli account utente di Windows.

Nota: Quando si utilizza il controllo accessi degli account utente, utilizzare lo stesso account di servizio usato per la configurazione delle *Procedure di installazione opzionali*. Per ulteriori informazioni, consultare la *Guida all'installazione di FreeFlow Core*.

Tabella 3.9 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
139, 445	SMB	In entrata: Recupera i file specificati nella preselezione dei componenti di un flusso di lavoro In uscita: Salva i file in directory condivise.
20, 21	FTP	In uscita: Recupera i file specificati nella preselezione dei componenti di un flusso di lavoro
80	HTTP	In uscita: I file possono essere crittografati in cartelle attive. Nelle cartelle Windows condivise i file possono essere crittografati utilizzando il file system Windows o protetti utilizzando il controllo accessi degli account utente di Windows. Recupera i file specificati nella preselezione dei componenti di un flusso di lavoro.

Stampa Xerox® FreeFlow® Core

Xerox® FreeFlow® Core utilizza SNMP o HTTP con i comandi IPP o JMF per stabilire il tipo di DFE usando una connessione non crittografata. La stringa community SNMP pubblica della stampante o del DFE deve essere impostata sul valore predefinito. Se la stringa community SNMP pubblica della stampante o del DFE è stata modificata rispetto all'impostazione predefnita, assicurarsi che l'impostazione aggiornata sia registrata con FreeFlow Core. Assicurarsi che tutte le stampanti registrate con FreeFlow Core abbiano la stessa stringa community SNMP pubblica. Per istruzioni su come aggiornare la stringa community SNMP pubblica, consultare il documento "Note sulla versione di Xerox FreeFlow Core".

Un tipo di connessione non crittografata viene utilizzata nelle seguenti operazioni:

- Recupero dell'elenco delle code del DFE.
- Recupero del'elenco delle stampanti virtuali sul DFE EFI.
- Recupero delle funzionalità della stampante.
- Operazioni di lavoro sul DFE.
- Recupero delle informazioni sulla contabilità lavoro. Questa operazione non è applicabile per JMF.

Quando si è collegati a un'unità DFE configurata per supportare il protocollo IPP protetto, l'invio in stampa è crittografato. Per abilitare il protocollo IPP protetto, utilizzare l'opzione Stampa protetta nell'impostazione Stampante di destinazione. I dati tra FreeFlow Core e il DFE vengono criptati mediante la crittografia TLS 1.2 e SHA256.

Per abilitare l'invio in stampa a FreeFlow Print Server tramite il protocollo IPP protetto, procedere come segue:

1. Aggiungere un certificato a FreeFlow Print Server.
2. In Impostazione di Xerox® FreeFlow® Print Server, selezionare **Abilita SSL/TLS**.
3. Utilizzare il certificato Xerox® FreeFlow® Core per recuperare un certificato TLS/SSL da FreeFlow Print Server.

> **Nota:** Quando IPP protetto è configurato correttamente, viene visualizzato un messaggio `Certificate successfully installed` (Certificato installato correttamente).

FreeFlow Core non supporta la comunicazione al DFE tramite JMF protetto.

Tabella 3.10 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
161, 162	SNMP v1/v2	In uscita: Identifica il tipo di DFE durante l'impostazione di una stampante di destinazione ed il recupero del certificato.
80	HTTP	In uscita: Identifica il tipo di DFE durante l'impostazione di una stampante di destinazione ed il recupero del certificato.
N/A	ICMP	In uscita: Verifica la disponibilità del dispositivo prima del recupero del certificato
631	IPP v1.0/v1.1	In uscita: Invia lavori alle unità DFE, recupera lo stato dei lavori e invia i comandi lavoro all'unità DFE.
Porta JMF 8010 o definita per la stampante	JMF v1.3/v1.4	In uscita: Identifica il tipo di DFE durante la registrazione della stampante e invia il lavoro al DFE.
443	HTTPS	In uscita: Invia i lavori al DFE.

Xerox® FreeFlow® Core Cloud Print

La connessione tra il server Xerox® Freeflow® Core Cloud Print e il client è sempre crittografata e richiede l'installazione di un certificato CA. Tra il server FreeFlow Core Cloud Print e il client si utilizza TLS 1.2.

Per installare il certificato nel server, usare Gestione Internet Information Services (IIS). Per ulteriori informazioni, fare riferimento alla documentazione Windows.

Il client Xerox® FreeFlow® Core Cloud Print utilizza SNMP o HTTP per stabilire il tipo di DFE usando una connessione non crittografata. La stringa community SNMP pubblica della stampante o del DFE viene impostata sul valore predefinito.

La connessione tra il client Xerox® FreeFlow® Core Cloud Print e l'unità DFE non supporta il protocollo IPP protetto.

Tabella 3.11 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
161, 162	SNMP (v1/v2)	In uscita: Identifica il tipo di DFE durante l'impostazione di una stampante di destinazione
631	IPP (v1.0/v1.1)	In uscita: Invia lavori alle unità DFE, recupera lo stato dei lavori e invia i comandi lavoro all'unità DFE.
443	HTTPS	In ingresso nel server: Accetta le connessioni dal client Xerox® FreeFlow® Core Cloud Print In uscita nel client: Si connette al server Xerox® FreeFlow® Core Cloud Print
Porta JMF 8010 o definita per la stampante	JMF v1.3/v1.4	In uscita: Identifica il tipo di DFE durante la registrazione della stampante e invia il lavoro al DFE.

Notifica e-mail

Xerox® FreeFlow® Core è un client e-mail che si connette al server e-mail di un cliente. È possibile crittografare le notifiche e-mail e successivamente collegarsi a un server di posta che supporta la crittografia. SSL abilita la crittografia delle comunicazioni tra il servizio di notifica e il server SMTP.

Le credenziali crittografate vengono archiviate localmente.

Tabella 3.12 Configurazione del firewall

Porta	Protocollo o applicazione	Tipo di connessione del firewall
25, 2525, 465, 475, 587	SMTP	In uscita: Invia notifiche e-mail **Nota:** Il numero di porta richiesto e l'uso di una connessione protetta dipendono dalla configurazione del server SMTP.

Conformità FIPS

Xerox ® FreeFlow® Core viene eseguito su un sistema operativo Windows con conformità a FIPS 140-2 abilitata. Per abilitare la conformità FIPS, fare riferimento alla documentazione Microsoft. FreeFlow Core viene eseguito in modalità di conformità FIPS per impostazione predefinita.

FreeFlow Core disabilita il supporto per la crittografia DES e Triple DES.

Se è richiesta la stampa IPP con Autenticazione Digest, disabilitare la modalità di conformità FIPS. FreeFlow Core diventerà non conforme ai requisiti di crittografia.

Crittografia dati

Elaborazione dei file

FreeFlow Core non sottopone esplicitamente a crittografia i file inviati in elaborazione prima di memorizzare il file nel file system del PC.

Accesso all'account utente e Memorizzazione lavoro

Password degli account utente

È ammesso riutilizzare le password.

Blocco degli account utente

Se l'autenticazione di FreeFlow Core ha esito negativo, gli utenti non vengono bloccati dopo i tentativi non andati a buon fine.

Disconnessione dall'account utente

Gli utenti connessi vengono automaticamente disconnessi dopo 30 minuti di inattività. La durata del periodo di inattività non è configurata.

Attività degli account utente

Il registro di verifica degli accessi utente a FreeFlow Core non è disponibile.

Memorizzazione lavoro

Dopo l'elaborazione, il periodo di memorizzazione del lavoro in FreeFlow Core è di 24 ore.

La stampante FreeFlow Core è configurato per cambiare il periodo di memorizzazione prima che i lavori completati vengano rimossi automaticamente. Dopo 24 ore, il dispositivo FreeFlow Core rimuove i lavori completati.

Per rimuovere i lavori manualmente, utilizzare l'interfaccia utente grafica Web di FreeFlow Core.

4

Protezione

Questo capitolo contiene:

In Xerox, i problemi legati a sicurezza e protezione sono al centro dell'attenzione. In qualità di azienda leader nello sviluppo di tecnologie digitali, Xerox ha dimostrato il massimo impegno nel mantenere la sicurezza e la protezione delle informazioni digitali, identificando possibili vulnerabilità e attivandosi per limitare i rischi.

Xerox si impegna a offrire dispositivi software più sicuri possibile in base alle informazioni e alle tecnologie disponibili senza diminuire prestazioni, valore, funzionalità e produttività.

I componenti di Xerox® FreeFlow® Core vengono controllati per garantire la conformità agli standard di sicurezza utilizzando gli strumenti di scansione più usati disponibili in commercio. Xerox si impegna a risolvere le vulnerabilità rilevate in base ai risultati ottenuti da test condotti sulle applicazioni.

Xerox distribuisce bollettini sulla sicurezza quando richiesto. Queste informazioni vengono comunicate sulla pagina del sito Web relativa https://www.xerox.com/security, nella sezione relativa alle istruzioni sulla sicurezza dei prodotti. Il sito Web contiene informazioni aggiornate sullo stato stampante di vulnerabilità della sicurezza, white paper, standard di certificazione Common Criteria nonché informazioni sulla sicurezza McAfee Intel e un portale per inviare a Xerox domande in merito alla sicurezza.

Protezione da virus

Xerox adotta speciali precauzioni per garantire che il software venga fornito senza contaminazioni di virus informatici. Gli esperti IT consigliano Xerox come soluzione ottimale per un software di rilevamento virus. Per proteggere la stampante da virus, è assolutamente necessario che il software di rilevamento virus sia costantemente aggiornato.

Per migliorare le prestazioni è consigliabile escludere le cartelle di installazione di Xerox® FreeFlow® Core e SQL Server dalla scansione antivirus.

È possibile escludere i file seguenti dalle scansioni antivirus:

- <directory di installazione FreeFlow Core>\Logs
- <directory di installazione FreeFlow Core>\Platform\Logs
- <directory di installazione FreeFlow Core>\JobSubmit\Logs
- <directory di installazione FreeFlow Core>\Config
- <directory di installazione FreeFlow Core>\Platform\Config
- <Directory dei dati utente di FreeFlow Core>\
- Le cartelle all'esterno della directory dei dati utente di FreeFlow Core usate da FreeFlow Core

5

Aggiornamento software

È consigliabile mantenere costantemente aggiornati tutti i dispositivi software installati nel server Xerox® FreeFlow® Core. Eseguire Microsoft Windows Update almeno una volta al mese.

Sul sito https://www.support.xerox.com/support/core/software/enus.html sono disponibili gli aggiornamenti software di FreeFlow Core. I clienti possono installare direttamente l'aggiornamento software.