VERSIONE 8.0.0
AGOSTO 2024
702P09306

Xerox® FreeFlow® Core

Guida alla sicurezza

BR40387

Sommario

Panoramica

Questo capitolo contiene:

Finalità

Lo scopo di questa Guida alla sicurezza è divulgare informazioni in materia di sicurezza del prodotto relative a Xerox® FreeFlow® Core. In questo contesto, la sicurezza del prodotto è definita come il modo in cui i dati vengono archiviati e trasmessi, come si comporta il prodotto in un ambiente di rete e come effettuare l'accesso al prodotto localmente e in remoto. Questo documento descrive la progettazione, le funzioni e le caratteristiche di Xerox® FreeFlow® Core rispetto alla sicurezza delle informazioni (IA - Information Assurance), nonché alla tutela dei dati sensibili dei clienti.

Questo documento non fornisce informazioni a livello di tutorial riguardo alla sicurezza e alla connettività delle caratteristiche e funzionalità di Xerox® FreeFlow® Core. Per maggiori informazioni su tali caratteristiche e funzioni, consultare la *Guida di Xerox® FreeFlow® Core*. Si presume che l'utente abbia una conoscenza pratica di questi argomenti.

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

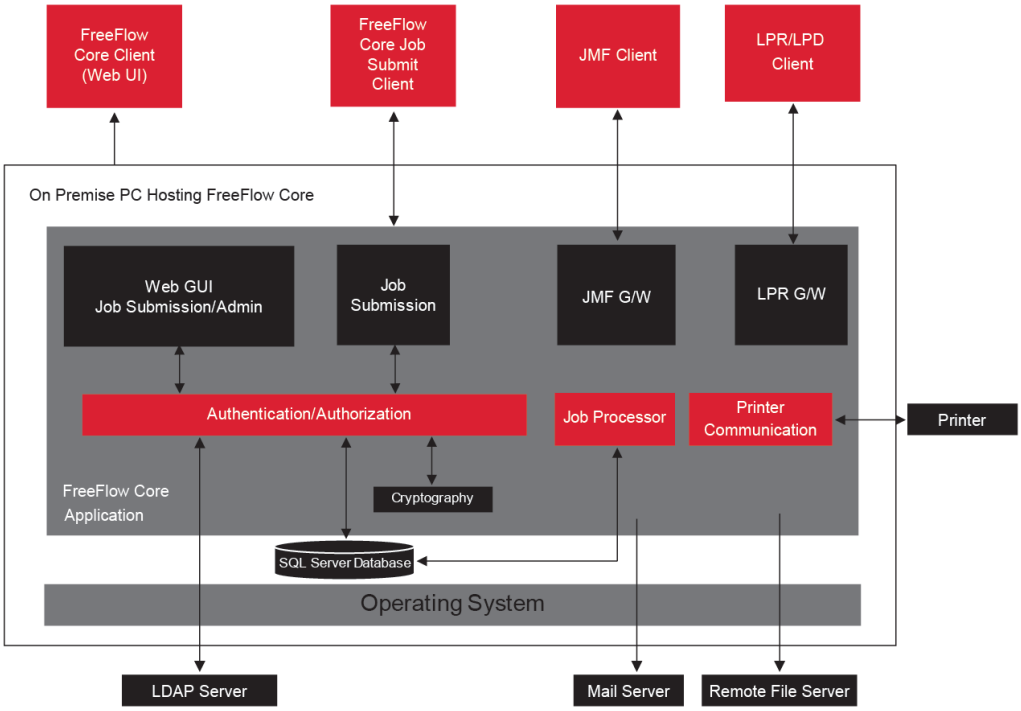
Le informazioni contenute in questo documento sono accurate alla data della sua pubblicazione. Dette informazioni vengono fornite senza alcuna garanzia. In nessuna circostanza Xerox® Corporation sarà ritenuta responsabile per danni risultanti dall'utilizzo o mancato utilizzo delle informazioni fornite 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.

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.

Struttura del software di sistema



Aspetti legati alla sicurezza di alcune funzioni

Questo capitolo contiene:

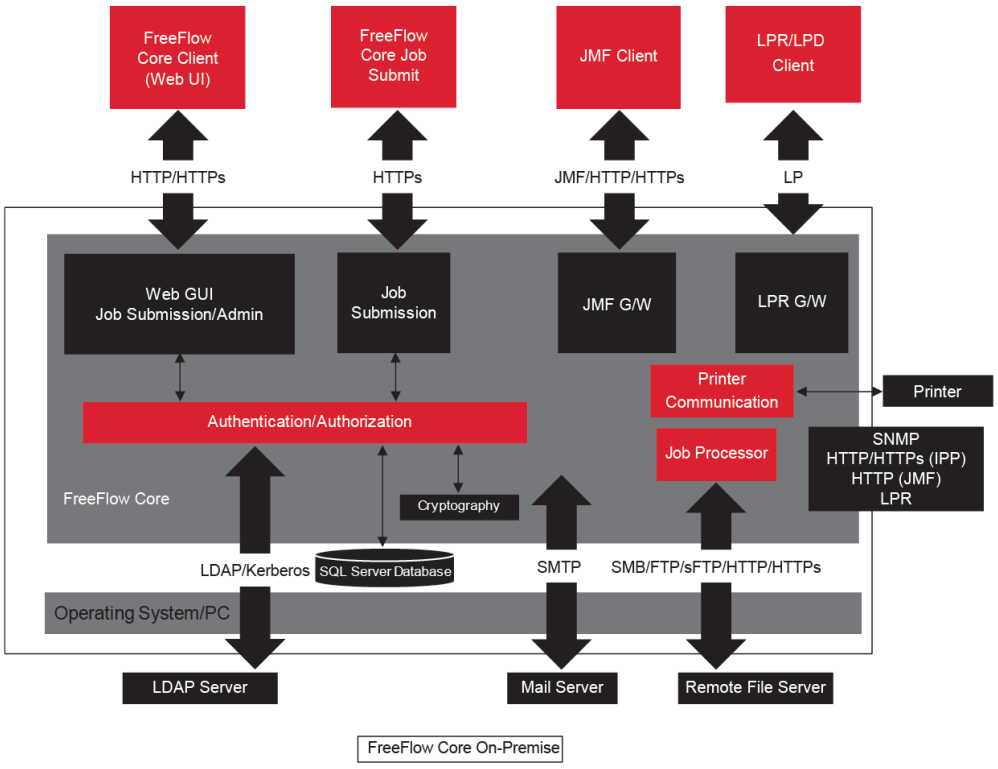
Accesso al sistema

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 server a IIS (Internet Information Services). Seguire le indicazioni disponibili nella documentazione Windows.
- Se le connessioni HTTPS sono abilitate, è necessario configurare l'impostazione di richiesta SSL su Microsoft Internet Information Service (IIS). Dal prompt dei comandi di Windows, eseguire il file batch RequireSSL, reperibile nella directory denominata Support all'interno della directory di installazione di FreeFlow Core o in `C:\Program Files\Xerox\FreeFlow Core`.
- FreeFlow Core supporta i protocolli di crittografia TLS.

Nota: FreeFlow Core utilizza le impostazioni del sistema operativo che supportano il protocollo TLS. Per assicurarsi di utilizzare le versioni correnti dei protocolli di crittografia, si raccomanda che il sistema operativo esegua gli aggiornamenti più recenti.

- 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 sistema 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 vengono bloccati dall'applicazione dopo tre tentativi di accesso non riusciti.

Nota: Per ulteriori impostazioni account utente, fare riferimento a Accesso all'account utente e Memorizzazione lavoro. Le impostazioni vengono configurate dall'amministratore di FreeFlow Core.

Per assegnare i ruoli agli utenti, consultare la sezione *Impostazione dell'accesso utente* della *Guida di Xerox® 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:
  - Cartella attiva
  - Notifiche
  - Accesso utente
  - Regione
  - Protezione
  - Rapporti Core
  - Scambio Core
  - Opzioni coda
  - Licenza Core
- Utilità del server Core disponibili sul desktop del server:
  - Scambio FreeFlow® Core
  - Configurazione FreeFlow® Core
  - Rapporti FreeFlow® Core per l'utilità riga di comando

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

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 non sono crittografate quando si utilizza HTTP. Per una trasmissione sicura, abilitare HTTPS e la richiesta di SSL su IIS per un accesso sicuro tramite browser Web a Xerox® FreeFlow® Core.

- Se si esegue l'autenticazione degli utenti tramite Xerox® FreeFlow® Core, le informazioni degli utenti vengono decrittografate. Le credenziali vengono archiviate localmente e crittografate.
- 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.
- È possibile configurare l'autenticazione Xerox® FreeFlow® Core per utilizzare una Windows Active Directory esistente. Questa configurazione utilizza le credenziali desktop dell'utente corrente come credenziali di accesso per il client Xerox® FreeFlow® Core.

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.
389636 3268 3269	LDAPLDAP TLS LDAP GC LDAP GC TLS	In uscita: Convalida i gruppi AD durante la configurazione dell'autenticazione di 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 Xerox® 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, HTTPS, FTP o sFTP.

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 istruzioni aggiornate sull'abilitazione della conversione da Office, consultare il documento *Note di rilascio di Xerox® FreeFlow® Core*. Per scaricare il documento, accedere alla pagina Web di FreeFlow® Core all'indirizzo http://xerox.com/automate. In cima alla pagina, fare clic su **Risorse proprietario**, quindi fare clic su **Note di rilascio** in cui vengono illustrati i requisiti completi del sistema.

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
443	HTTPS	In uscita: Recupera i file utilizzando l'URL HTTPS elencato nel manifest
22	sFTP	In uscita: Recupera i file utilizzando l'FTP sicuro elencato nel 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
da 721 a 731	LPR	In uscita: Invia le richieste LPR a una stampante che supporta LPD.

Segnali di stato stampante e comandi JMF

Segnali e comandi JMF (Job Messaging Format) a un client JMF supportano le connessioni protette. Il recupero dei file JMF supporta le connessioni HTTPS.

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

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/FreeFlowCore`. 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

Nodi del flusso di lavoro

I componenti del flusso di lavoro che recuperano o salvano i file di lavoro possono usare unità mappate, percorsi di file UNC, URI HTTP, HTTPS o FTP. L'URI sFTP supporta il recupero dei file di lavoro come MAX, JMF.

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 Xerox® FreeFlow® Core*.

Tabella 3.8 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: Recupera i file specificati nella preselezione dei componenti di un flusso di lavoro
443	HTTPS	In uscita: 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, JMF o XBDS 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 predefinita, 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.
- Invio di un lavoro di stampa a una stampante utilizzando LPR.

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 e

SHA256.

Abilitazione di un invio in stampa al Server di stampa FreeFlow tramite il protocollo IPP protetto

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

1. Aggiungere un certificato TLS al Server di stampa FreeFlow.
2. Selezionare **Abilita TLS** nell'impostazione del Server di stampa Xerox® FreeFlow®.
3. Utilizzare il certificato Xerox® FreeFlow® Core per recuperare il certificato TLS dal Server di stampa FreeFlow.

Nota: una volta portata a termine correttamente la configurazione IPP protetta, viene visualizzato il messaggio: `Certificato installato con successo .`

Abilitazione di un invio in stampa a Fiery tramite il protocollo IPP protetto

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

1. Per avviare l'interfaccia utente di Fiery, inserire l'indirizzo IP di Fiery in un qualsiasi browser Web.
2. Selezionare **Configura Fiery** nel riquadro a sinistra.
3. Accedere con le credenziali del controller Fiery.
4. Selezionare **Sicurezza**, quindi creare il certificato autofirmato o inserire i dati con i certificati della CA.
5. Abilitare **SSL\TLS** nella schermata di configurazione dell'interfaccia utente.
6. Quando SSL\TLS è abilitato, viene visualizzato un messaggio di conferma che indica di riavviare il controller.
7. Selezionare **Sì**.
8. Avviare l'**utilità Windows Configurazione Core** in Xerox® FreeFlow® Core.
9. Selezionare la scheda **Certificato Core**, fornire l'indirizzo IP del controller Fiery e selezionare **Recupera certificato**.

   Viene visualizzato il messaggio `Certificato installato correttamente`.
10. Configurare la stampante in Xerox® FreeFlow® Core con l'opzione di stampa protetta nella schermata Gestione stampante.

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

Tabella 3.9 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 entrata: La stampante JDF recupera il file di stampa utilizzando HTTP.

PORTA	PROTOCOLLO O APPLICAZIONE	TIPO DI CONNESSIONE DEL FIREWALL
		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.
4004	JMF	In entrata: Riceve il messaggio JMF `ReturnQueueEntry` dalla stampante
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 un lavoro al DFE.
443	HTTPS	In uscita: Comunicazione della stampante con il DFE
515, da 721 a 731	LPR	In uscita: Invia le richieste LPR a una stampante che supporta LPD

Notifica e-mail

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

Le credenziali crittografate vengono archiviate localmente.

Tabella 3.10 Configurazione del firewall

PORTA	PROTOCOLLO O APPLICAZIONE	TIPO DI CONNESSIONE DEL FIREWALL
25, 465, 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 e GDPR

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.

FreeFlow Core è conforme al Regolamento generale sulla protezione dei dati dell'UE (GDPR).

Salvaguardia della sicurezza generale

AUTENTICAZIONE DI ACCOUNT DI SERVIZIO, UTILITÀ E INTERFACCIA DELLA RIGA DI COMANDO (CLI)

Gli account di servizio, le utilità e la CLI di FreeFlow Core ora utilizzano l'autenticazione Windows. Ciò si ottiene aggiungendo l'account di servizio o l'account utente attualmente connesso a un gruppo Windows locale denominato Sicurezza FreeFlow Core. Per ulteriori informazioni, consultare il documento *Xerox FreeFlow Core – Note sulla versione*.

PROTEZIONE DEI DATI UTENTE

Sicurezza di documenti e file

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

Il contenuto di origine del documento contiene dati di identificazione personale (PII) o altri contenuti riservati. Pertanto, è responsabilità dell'utente gestire i dati digitali in conformità alle migliori prassi di protezione dei dati.

Dati di identificazione personale (PII)

Quando ci si registra per ottenere una licenza del software FreeFlow Core, vengono raccolto dati PII. Tali dati sono:

- Nome società
- Chiave di attivazione e numero di serie
- ID hist/UUID sistema
- Nome utente
- Indirizzo (Via, Città, Provincia, CAP, Paese)
- Indirizzo e-mail: (facoltativo)

Tali dati vengono trasmessi in modo sicuro all'host licenze di Xerox.

I dati PII, in particolare l'indirizzo e-mail dell'utente che viene utilizzato per il recupero della password, vengono archiviati nel sistema FreeFlow Core. I dati sono crittografati.

Accesso all'account utente e Memorizzazione lavoro

PASSWORD DEGLI ACCOUNT UTENTE

Il riutilizzo di una password è consentito fino a 10 volte. Il numero di volte in cui una password può essere riutilizzata è configurabile.

BLOCCO DEGLI ACCOUNT UTENTE

Se l'autenticazione non riesce utilizzando Xerox FreeFlow Core Client, gli utenti vengono bloccati dopo tre tentativi di accesso non riusciti per 30 minuti. Il numero di tentativi di accesso non riusciti e la durata del blocco sono configurabili.

DISCONNESSIONE DALL'ACCOUNT UTENTE

Dopo 30 minuti di inattività, gli utenti che hanno effettuato l'accesso a Xerox® FreeFlow® Core Client vengono disconnessi automaticamente. La durata del periodo di inattività è configurabile.

ATTIVITÀ DEGLI ACCOUNT UTENTE

Il registro di controllo delle transazioni di accesso dell'utente a FreeFlow Core si trova in Visualizzatore eventi Windows, nella sezione **Applicazione** della cartella **Registri di Windows**.

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.

PROPRIETÀ LAVORO

Abilita la limitazione allo scaricamento di file trovati in Proprietà lavoro per un lavoro visualizzato in Stato e gestione lavori di FreeFlow Core.

Diritti di account utente

Per configurare l'account di servizio Xerox® FreeFlow® Core è possibile usare un account amministratore locale o un account non amministratore. Quando si utilizza un account appartenente al gruppo di amministratori locali, non sono richieste azioni speciali.

Quando si utilizza un account non amministratore, sono necessari ulteriori diritti, oltre ai diritti del gruppo di utenti standard. FreeFlow® Core Configure aggiunge automaticamente gli ulteriori diritti, come elencato nella seguente tabella:

IMPOSTAZIONE CRITERI DI GRUPPO	NOME DELLA COSTANTE
Agisci come parte del sistema operativo	SeTcbPrivilege
Regola le quote di memoria per un processo	SeIncreaseQuotaPrivilege
Consenti l'accesso locale	SeInteractiveLogonRight
Esegui il backup dei file e delle directory	SeBackupPrivilege
Crea un oggetto token	SeCreateTokenPrivilege
Crea oggetti globali	SeCreateGlobalPrivilege
Crea oggetti condivisi permanenti	SeCreatePermanentPrivilege
Esegui il debug dei programmi	SeDebugPrivilege
Carica e scarica i driver di dispositivo	SeLoadDriverPrivilege
Accedi come processo batch	SeBatchLogonRight
Accedi come servizio	SeServiceLogonRight
Gestisci file registro di controllo e di protezione	SeSecurityPrivilege
Esegui attività di manutenzione volume	SeManageVolumePrivilege
Creazione di profilo del singolo processo	SeProfileSingleProcessPrivilege
Creazione di profilo delle prestazioni del sistema	SeSystemProfilePrivilege
Sostituisci un token a livello di processo	SeAssignPrimaryTokenPrivilege

Nota: I diritti elencati nella tabella sono definiti in https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment.

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. Xerox consiglia di installare il software di rilevamento virus e di rilevamento e prevenzione di intrusione negli endpoint sul server FreeFlow Core. Questo software e il sistema operativo vengono aggiornati con le ultime patch di sicurezza, come consigliato dai rispettivi fornitori.

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

Aggiornamento software

Xerox non è responsabile dello stato del sistema operativo che gestisce Xerox® FreeFlow® Core. È responsabilità del cliente mantenere il sistema aggiornato e assicurarsi che sia configurato correttamente e dotato delle patch appropriate. Eseguire l'aggiornamento di Microsoft® Windows® almeno una volta al mese.

Quando si eseguono gli aggiornamenti di Windows, utilizzare l'opzione **Windows Update** per implementare l'aggiornamento. Si raccomanda di non installare aggiornamenti in anteprima opzionali, in quanto possono compromettere l'affidabilità del server Xerox® FreeFlow® Core.

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.

Informazioni e risorse aggiuntive

Xerox e la sicurezza

Xerox gestisce una pagina Web pubblica aggiornata che contiene le ultime informazioni in merito alla sicurezza dei suoi prodotti. Consultare www.xerox.com/security.

Risposte a vulnerabilità note

Xerox ha creato un documento che descrive in dettaglio la "Politica di divulgazione e gestione delle vulnerabilità di Xerox" utilizzata per l'individuazione e la risoluzione delle vulnerabilità nei componenti software e hardware di Xerox. È possibile scaricare il documento dalla seguente pagina: https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html.

Risorse aggiuntive

RISORSE SULLA SICUREZZA	URL
Domande frequenti sulla sicurezza	www.xerox.com/en-us/information-security/frequently-asked-questions
Bollettini, avvisi e aggiornamenti sulla sicurezza	www.xerox.com/security
Archivio delle notizie sulla sicurezza	security.business.xerox.com/en-us/news/
Xerox Trust Center	https://trust.corp.xerox.com/