Remote Services @ Xerox

Whitepaper sulla sicurezza

Versione 4.0

Marzo 2022

IS 614672/IS 514590

Indice generale

1. Scopo generale e pubblico

Il whitepaper sulla sicurezza di Remote Services @Xerox viene fornito per aiutare i clienti a comprendere e implementare la soluzione di servizi remoti sicuri più adatta alla struttura delle loro reti e alle politiche di sicurezza delle informazioni. Per garantire il metodo di configurazione più sicuro, potrebbero essere necessarie modifiche al firewall Internet, ai server proxy Web o ad altre infrastrutture di rete correlate alla sicurezza del cliente.

Il pubblico di destinazione di questo documento include fornitori tecnici, gestori di rete e professionisti della sicurezza di rete interessati alle funzionalità dei servizi remoti e all'implementazione della sicurezza di tali funzionalità.

Si consiglia di rivedere il documento nella sua interezza per certificare l'uso dei prodotti e dei servizi Xerox® all'interno dell'ambiente di rete di un cliente.

2. Proposta di valore

Offriamo un modo sicuro e protetto per inviare i dati della periferica al nostro sistema certificato ISO per automatizzare le attività comuni e fornire un servizio e un'esperienza di supporto migliori.

- La segnalazione dei contatori di fatturazione è automatizzata e accurata.
- Il programma di rifornimento automatico delle forniture fornisce il toner in base ai livelli di toner riportati della stampante, quindi non è necessario tenere traccia dell'inventario o richiedere forniture.
- L'invio di informazioni diagnostiche ci consente di supportare meglio la tua periferica, spesso consentendo una risoluzione dei problemi più rapida.
- Alcuni modelli di stampante possono verificare la presenza di importanti aggiornamenti software e installarli a livello di programmazione senza l'intervento del cliente.Vedere la nota
- Le funzionalità dei nostri servizi di gestione forniscono anche un modo per gestire stampanti non a marchio Xerox, oltre alle stampanti a marchio Xerox.
- Questi servizi consentono ai nostri clienti un uso più efficiente del loro tempo.

Tutto questo è fatto tenendo sempre in mente la sicurezza.

Nota: questa opzione può essere disabilitata per gli ambienti in cui i clienti certificano una versione del software impostata e desiderano controllare il software di stampa quando si verificano gli aggiornamenti. Ciò può essere fatto senza dover disabilitare le restanti funzionalità dei servizi remoti.

3. Remote Services

Le informazioni sono una risorsa chiave e la sicurezza è fondamentale per tutte le risorse organizzative, incluse le periferiche di stampa multifunzione in rete (MFP). Oggi, gestire un parco di periferiche di stampa multifunzione garantendo un livello di sicurezza accettabile presenta una serie di sfide uniche che spesso vengono trascurate. Comprendiamo questa complessità e rispondiamo alle esigenze di sicurezza dei nostri clienti. I prodotti Xerox®, i sistemi Xerox® e le offerte di servizi remoti sono progettati per integrarsi in modo sicuro con i flussi di lavoro esistenti dei nostri clienti utilizzando le tecnologie sicure più recenti.

Per impostazione predefinita, nessuna immagine del cliente da stampa, fax, scansione, azioni di copia o altre informazioni sensibili viene trasmessa ai nostri server.

I server Xerox con sede negli Stati Uniti sono conformi ai rigorosi requisiti di sicurezza per la gestione della sicurezza delle informazioni. I nostri datacenter e applicazioni di servizi remoti sono sempre conformi ai requisiti annuali della Dichiarazione sugli standard per l'attestazione (SSAE) No-16, Sarbanes-Oxley Act (SOX) e sono certificati ISO 27001:2013.

4. Modelli di distribuzione

I clienti possono scegliere tra i seguenti modelli di distribuzione Xerox® Remote Services, ugualmente sicuri:

- **Modello Combination** – ***(Modello preferito)*** L'implementazione congiunta del modello Device Direct e con applicazioni Device Management è ideale in quanto fornisce il set di dati e le capacità di gestione delle periferiche più validi.

- **Modello Device Direct** - Device Direct consente alle periferiche di stampa di comunicare direttamente con i server di comunicazione Xerox® remoti via Internet attraverso il firewall del cliente per supportare il rifornimento automatico (ASR), le letture automatiche dei contatori (AMR) e la segnalazione diagnostica delle periferiche.Questo modello di distribuzione fornisce una serie di elementi di dati nel carico utile standard in modo da includere errori di periferiche, avvisi, contatori, elementi di servizio ad alta frequenza (HFSI, High Frequency Service Items) e altri attributi della periferica di stampa.
- **Modello con applicazioni Device Management** - Le applicazioni Device Management Xerox® possono essere implementate nella rete di un cliente per raccogliere una serie di attributi di dati dalle periferiche di stampa per supportare anche ASR (Automatic Supplies Replenishment), AMR (Automatic Meter Reads) e report di diagnostica delle periferiche.Gli attributi delle periferiche di stampa vengono raccolti e quindi trasmessi in modo sicuro ai server Xerox remoti.Gli attributi dei dati delle periferiche di stampa Xerox e non Xerox possono essere comunicati come parte di questo modello di distribuzione.

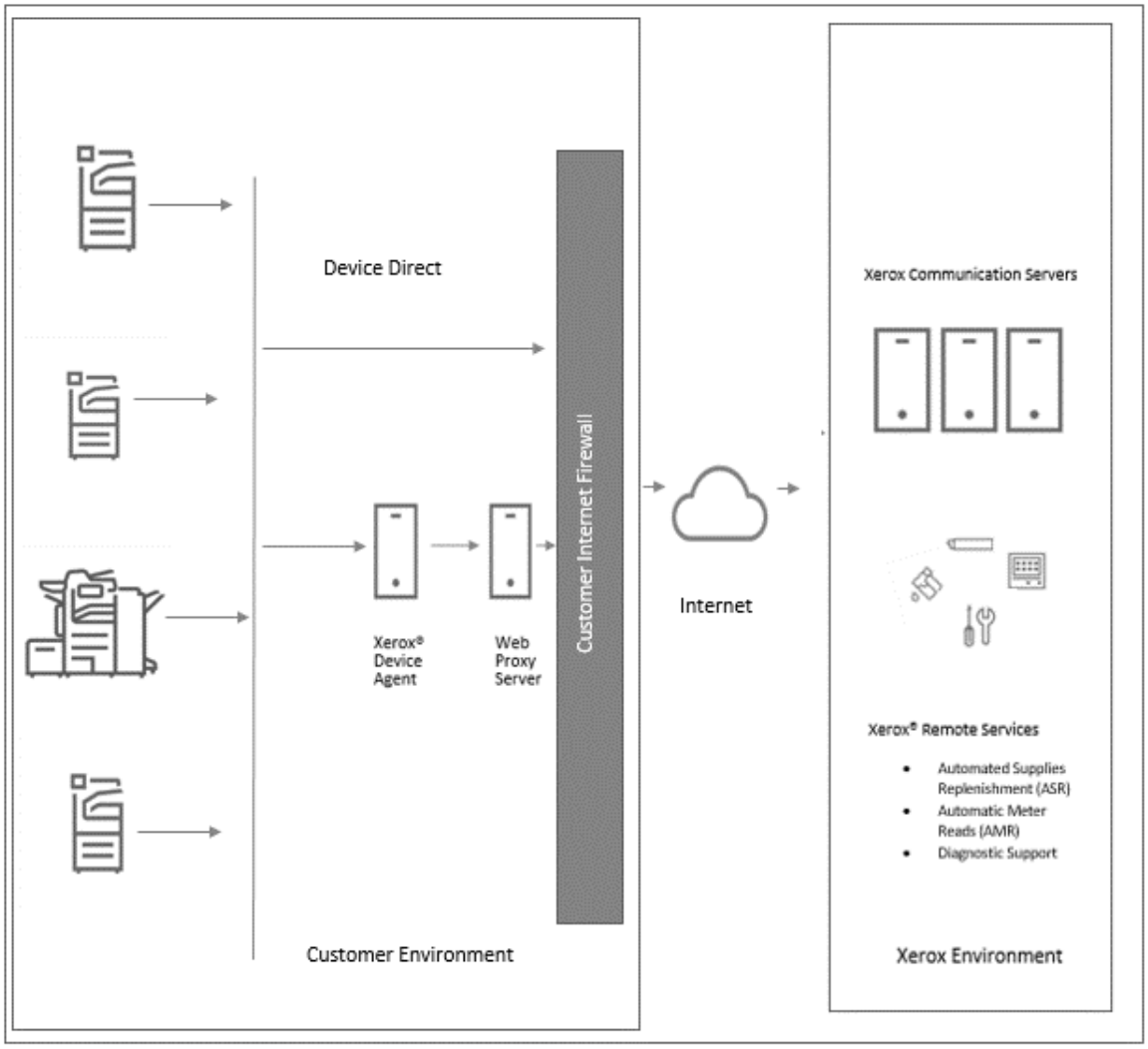
Tutti i modelli di implementazione per Xerox® Remote Services sono ugualmente sicuri e sfruttano i più recenti protocolli e porte basati sul Web standard del settore per stabilire un canale sicuro e crittografato quando si trasmettono gli attributi delle periferiche di stampa esternamente ai server Xerox remoti situati all'interno dei nostri data center protetti ridondanti.

Il modello di distribuzione scelto dipende dal tipo di soluzione di servizio di stampa dei nostri clienti, dalle politiche di sicurezza delle informazioni e dalle regole per la gestione della trasmissione degli attributi dei dati della periferica di stampa.

Modello di distribuzione Combination (preferito)

La distribuzione combinata viene implementata quando un cliente acquista più tipi di contratti di manutenzione Xerox per le proprie periferiche di stampa per ottenere una soluzione di servizi remoti più completa. Quando una periferica di stampa Xerox® viene inizialmente installata in una rete, il comportamento predefinito dei servizi remoti Xerox prevede che la periferica tenti automaticamente di comunicare in uscita con i nostri server di comunicazione utilizzando un metodo di connessione sicuro e autenticato.

Figura 1



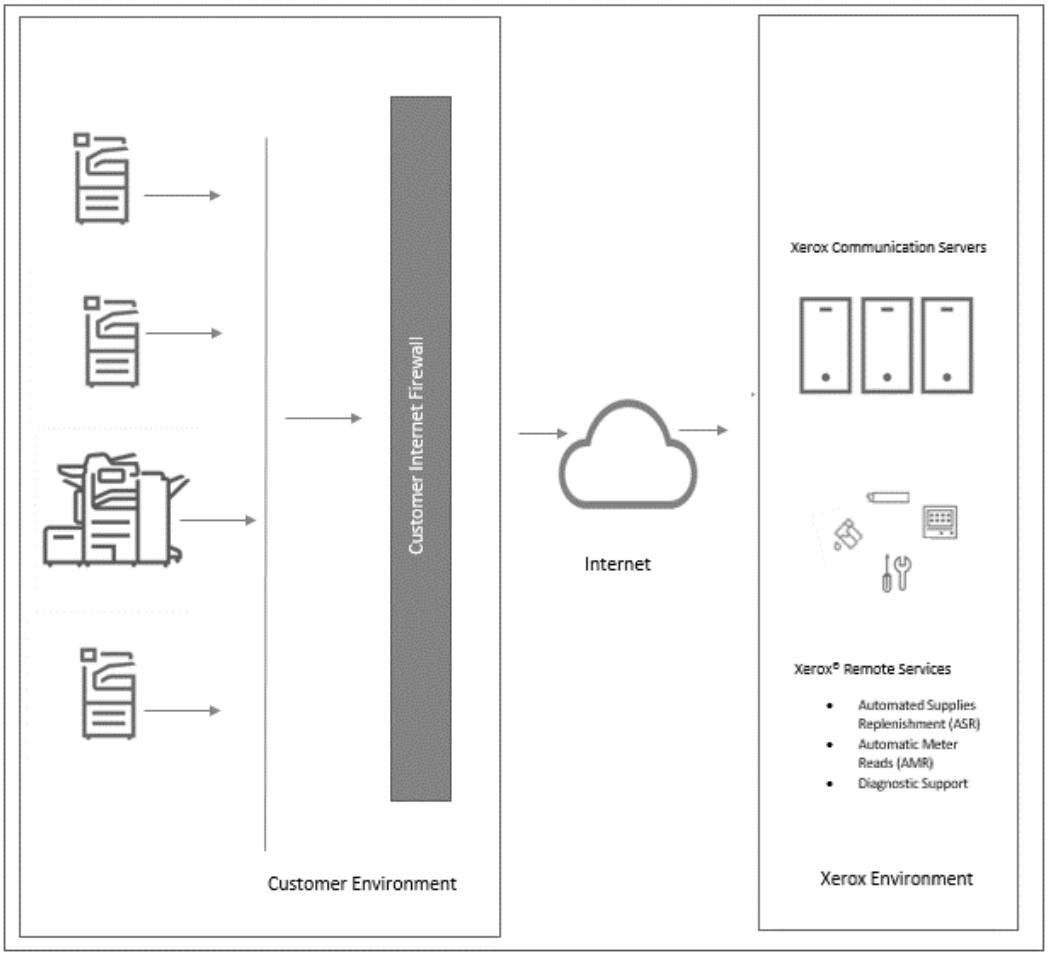
Combination Deployment Model

Modello di distribuzione Device Direct

Le periferiche Xerox® compatibili con Remote Services utilizzano una connessione di protocollo Transport Layer Security (TLS) 1.2 sulla porta standard sicura 443 per comunicare in uscita con i nostri server sicuri.

- Le periferiche di stampa all'interno dell'ambiente del cliente avviano tutte le comunicazioni con i server di comunicazione. Per abilitare la comunicazione sono necessarie le configurazioni standard del firewall sul sito.
- È necessario utilizzare un URL valido per i server di comunicazione (*.xerox.support.com) per autenticare le periferiche di stampa nell'infrastruttura Xerox
- La periferica richiede una registrazione con i server di comunicazione utilizzando le credenziali appropriate di autenticazione del certificato.
- I server di comunicazione convalidano le credenziali fornite dalle stampanti e accettano le richieste.
- I server di comunicazione sono protetti da un firewall e non sono accessibili da Internet.

Figura 2



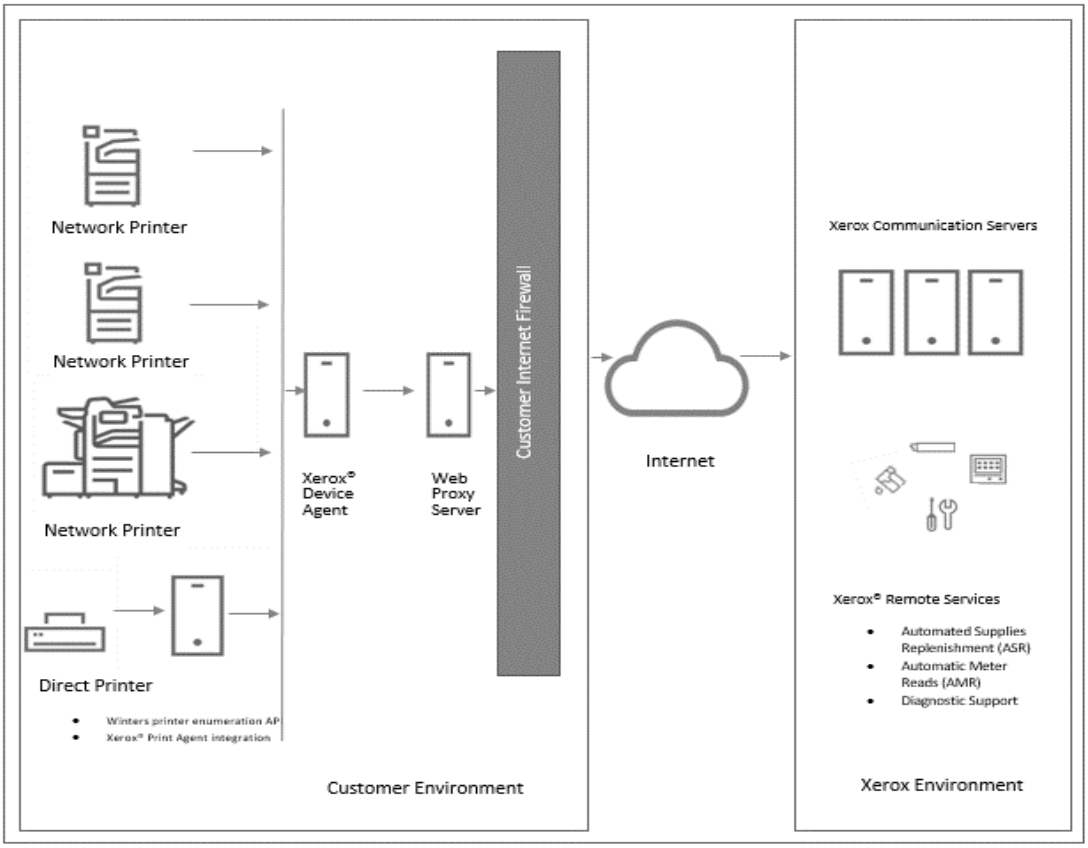
Device Direct Deployment Model

Modello di distribuzione con applicazioni Device Management

Le applicazioni Device Management (cioè **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **e Xerox Device Manager)** utilizzano una connessione con protocollo Transport Layer Security (TLS) 1.2 sulla porta standard sicura 443 per comunicare esternamente con i server di comunicazione.Vengono sfruttate ulteriori funzioni sonoper migliorare la sicurezza su questo canale e sono stabilite durante l'installazione iniziale delle applicazioni Device Management, che includono:

- L'applicazione Device Management all'interno dell'ambiente del cliente avvia tutte le comunicazioni con i server di comunicazione. Per abilitare la comunicazione sono necessarie le configurazioni standard del firewall sul sito.
- I server di comunicazione sono protetti da un firewall e non sono accessibili da Internet.
- L'applicazione Device Management richiede una registrazione con i server remoti utilizzando le credenziali appropriate di autenticazione dei certificati.
- I server di comunicazione convalidano le credenziali fornite dalle stampanti e accettano le richieste.
- L'applicazione Device Management autentica i server di comunicazione e attiva il servizio.

Figura 3



Device Management Application Deployment Model

5. Trasmissione dati e carichi utili

Fonti di dati

Gli attributi dei dati dell'unità di stampa inviati come parte del carico utile trasmesso provengono dalle seguenti fonti:

- Stampanti di rete Xerox® Office
- Stampanti di rete non Xerox
- Stampanti Xerox® Production
- Applicazioni Xerox® Device Management

Nota: non tutte le stampanti Xerox Office e Xerox Production supportano Xerox Remote Services. Puoi trovare un elenco completo dei prodotti idonei qui.Gli attributi delle periferiche di stampa variano a seconda del prodotto e della soluzione di distribuzione di Xerox® Remote Services.

Periferiche Xerox® Office

Tabella 1 Identifica gli attributi dei dati delle periferiche che possono essere trasmessi per i prodotti Xerox® Office compatibili con Remote Services.

Attributi dei dati	Descrizione dettagliata degli attributi dei dati
Identità della periferica di stampa	Include modello, livelli firmware del modulo, numeri di serie del modulo, date di installazione del modulo, dati di licenza e posizione, se disponibile.
Indirizzo di rete della periferica di stampa	Include l'indirizzo MAC (Media Access Control) e l'indirizzo di sottorete.
Proprietà della periferica di stampa	Include configurazione dettagliata dei componenti hardware, configurazione dettagliata dei moduli software, funzionalità/servizi supportati, ecc.
Stato della periferica di stampa	Include stati attivi, conteggi della cronologia guasti, registro eventi DFE, cronologia di trasmissione dati
Contatori della periferica di stampa	Include contatori di fatturazione, contatori relativi alla stampa, contatori relativi alla copia, contatori relativi a lavori di grandi dimensioni, contatori specifici per la produzione, contatori relativi a scansione-destinazione su modelli di produzione di fascia bassa, ecc.
Materiali di consumo della periferica di stampa	Include produttore, modello, numero di serie, nome, tipo, livello, capacità, stato, contatori durata, ecc.
Uso dettagliato della macchina di stampa	Include dati HFSI, dati NVM, sostituzione delle parti, registri DFE, dati diagnostici dettagliati, risoluzione dei guasti.
Dati tecnici/Debug	Include dati dettagliati non strutturati relativi al debug destinati esclusivamente all'utilizzo del supporto di 3° livello.
Dati correlati al lavoro del cliente	I prodotti di stampa Xerox® Production offrono la possibilità di riprodurre i dati relativi al lavoro a supporto di scenari di assistenza in escalation a Xerox tramite PostScript crittografato. Il cliente può controllare se attivare o meno questa funzione. Se il cliente sceglie di ritrasmettere a Xerox dati relativi al lavoro (ad es. PostScript crittografato), tali dati vengono gestiti in conformità con le politiche e gli standard di sicurezza delle informazioni (IS) di Xerox.

Le nostre periferiche di stampa di classe office trasmettono gli attributi dei dati della periferica in formato XML (eXtensible Markup Language) utilizzando un file compresso .zip. Una volta autenticato, ogni file viene quindi trasmesso tramite un canale crittografato ai server di comunicazione.

Periferiche Xerox® Production

Tabella 2 Identifica gli attributi dei dati della periferica che possono essere trasmessi per i prodotti Xerox® Production compatibili con Remote Services.

	Descrizione
Identità della periferica di stampa	Include modello, livello del firmware, numeri di serie del modulo e data di installazione.
Indirizzo di rete della periferica di stampa	Include l'indirizzo MAC (Media Access Control) e l'indirizzo di sottorete.
Proprietà della periferica di stampa	Include configurazione dettagliata dei componenti hardware, configurazione dettagliata dei moduli software, funzionalità/servizi supportati, modalità di risparmio energetico, ecc.
Stato della periferica di stampa	Include lo stato generale, avvisi dettagliati, cronologia degli ultimi 40 guasti, dati di inceppamento, ecc.
Contatori della periferica di stampa	Include contatori di fatturazione, contatori relativi alla stampa, contatori relativi alla copia, contatori relativi al fax, contatori relativi a lavori di grandi dimensioni, contatori relativi a scansione-destinazione, statistiche di utilizzo, ecc.
Materiali di consumo della periferica di stampa	Include nome del materiale di consumo, tipo (ad es. creazione immagine, finitura, supporti cartacei), livello, capacità, stato, dimensioni, ecc.
Uso dettagliato della macchina di stampa	Include contatori dettagliati relativi alla stampa, stati di accensione, quantità di sostituzione dettagliate delle unità sostituibili dal cliente (CRU), dati e distribuzioni dettagliati dei guasti CRU, utilizzo della funzione OCR (Optical Character Recognition) incorporata, distribuzione della lunghezza di stampa, distribuzione dell'utilizzo del vassoio della carta, supporti installati, distribuzione dei tipi di supporti, distribuzione delle dimensioni dei supporti, distribuzione della lunghezza del documento, numero di set, dati HFSI, dati NVM, distribuzione, conteggi dei pixel contrassegnati, copertura media dell'area per colore, errori/inceppamenti, contatori dettagliati relativi alla scansione.
Dati tecnici/Debug	Include informazioni di debug dettagliate che possono includere dati al di fuori del set di dati sopra elencato. Questi dati possono includere PII come nomi utente, indirizzi e-mail e dati di lavoro. Questi dati vengono inviati solo con l'esplicita autorizzazione del cliente e sono destinati esclusivamente all'uso del supporto per la risoluzione dei problemi in fase di escalation.

Le nostre periferiche di stampa di classe Production trasmettono gli attributi dei dati della periferica in formato XML (eXtensible Markup Language) utilizzando un file compresso .zip. Una volta autenticato, ogni file viene quindi trasmesso tramite un canale crittografato ai server dei servizi remoti.

Nota: il file e il contenuto dei dati identificati variano a seconda del modello di prodotto.

Applicazioni Xerox® Device Management

Sono disponibili diverse opzioni dell'applicazione Device Management in base all'ambiente di rete dei clienti e alle esigenze di gestione delle periferiche di stampa. Sono tutte ugualmente sicure e con valide capacità di gestione delle periferiche di stampa.

Di seguito è riportato un elenco di applicazioni di gestione unità: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition e Xerox Device Manager.

Ogni applicazione viene sincronizzata, per impostazione predefinita, almeno quotidianamente con i server di comunicazione protetti. Per garantire la massima sicurezza dei dati, i server di comunicazione sono ospitati in una struttura conforme alla norma ISO 27001. I dati inviati sono principalmente contatori di fatturazione specifici della stampante, livelli di fornitura e avvisi della stampante. I dati sono compressi, crittografati e protetti da diversi meccanismi:

- L'applicazione Xerox Device Management avvia tutti i contatti con i server di comunicazione Xerox; per abilitare la comunicazione sono necessarie le configurazioni firewall standard nell'ambiente del cliente.
- Le applicazioni Xerox Device Management richiedono un proxy valido, nel caso in cui sia richiesto un proxy per le comunicazioni Internet.
- I server di comunicazione Xerox si trovano dietro un firewall sicuro nell'ambiente Xerox e non sono accessibili da Internet.
- L'accesso all'interfaccia utente del server di comunicazione Xerox richiede l'autenticazione. Le informazioni sull'host dell'applicazione Xerox Device Management sono memorizzate in un account specifico per il sito del cliente e l'accesso a tali dati nei server di comunicazione Xerox è limitato agli account manager dei server di comunicazione Xerox.
- Tutte le comunicazioni del server di comunicazione Xerox sono registrate e disponibili per la visualizzazione.
- I dati inviati alle periferiche di stampa in rete, se abilitati, sono costituiti principalmente da comandi remoti che consentono a un amministratore del supporto account di richiedere l'esecuzione del livello di comando dell'applicazione Xerox Device Management durante gli scenari di supporto in escalation.
- Le richieste riguardano principalmente aggiornamenti del firmware, riavvii della stampante, stampa della pagina di prova e aggiornamenti dello stato corrente della periferica.
- L'applicazione Xerox Device Management esegue periodicamente il polling dell'account dei server di comunicazione Xerox per le richieste di comandi.
- I risultati delle operazioni derivanti dalle richieste di comando vengono inviati ai server di comunicazione Xerox, dove vengono quindi esaminati.

Nota: esiste un requisito di registrazione una tantum per l'installazione del software. Questa informazione per la registrazione include un campo per la posizione della periferica e l'e-mail di contatto.

Le applicazioni Xerox Device Management **(ad esempio Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition e Xerox Device Manager** trasmettono i dati degli attributi di stampa in formato XML (eXtensible Markup Language) utilizzando un file compresso .zip. Il file viene quindi crittografato e trasmesso tramite canali crittografati ai server di comunicazione remota.

La tabella 3 identifica un elenco di attributi e descrizioni dei dati del dispositivo che possono essere inviati tramite l'app Xerox® Device Mgmt.

Attributi dei dati	Descrizione dettagliata degli attributi dei dati
Identità della periferica di stampa	Include produttore, modello, descrizione, livello del firmware, numero di serie, tag dell'asset, nome del sistema, contatto, posizione, stazione di lavoro dello stato di gestione (desktop), numero di telefono fax e nome della coda.
Indirizzo di rete della periferica di stampa	Include indirizzo MAC, indirizzo IP, nome DNS, subnet mask, gateway IP predefinito, ultimo indirizzo IP noto, indirizzo IP modificato, fuso orario, indirizzo IPX, numero di rete esterna IPX, server di stampa IPX.
Proprietà della periferica di stampa	Include componenti installati, descrizioni dei componenti, funzioni/servizi supportati, velocità di stampa, supporto dei colori, opzioni di finitura, supporto duplex, tecnologia di marcatura, disco rigido, RAM, supporto della lingua, proprietà definite dall'utente.
Stato della periferica di stampa	Include stato generale, avvisi dettagliati, messaggi della console locale, stato del componente, dati relativi al recupero dello stato, data di rilevamento, metodo/tipo di rilevamento, tempo di attività della periferica, trap supportati/abilitati.
Contatori della periferica di stampa	Include contatori di fatturazione, contatori relativi alla stampa, contatori relativi alla copia, contatori relativi al fax, contatori relativi a lavori di grandi dimensioni, contatori relativi alla scansione, statistiche di utilizzo e volume di destinazione.
Materiali di consumo della periferica di stampa	Include nome del materiale di consumo, tipo (ad es. creazione immagine, finitura, supporti cartacei), livello, capacità, stato, dimensioni e attributi correlati
Utilizzo dettagliato della periferica di stampa	Dati di tracciamento del lavoro basati sull'utente, che includono: caratteristiche del lavoro (ID, nome del documento, proprietario, tipo di documento, tipo di lavoro, colore, duplex, supporto richiesto, dimensioni, pagine, set, errori), destinazione (periferica di stampa, modello, nome DNS, indirizzo IP, indirizzo MAC, numero di serie), risultati della stampa del lavoro (tempo di invio, tempo di stampa del lavoro, pagine stampate, pagine a colori/in bianco e nero, modalità colore utilizzata, N-up), dati di contabilizzazione (codice di riaddebito, prezzo di riaddebito, fonte di contabilizzazione), origine del lavoro di stampa (stazione di lavoro, nome del server di stampa/indirizzo MAC, nome della coda, porta, nome utente, ID utente), dati di gestione Xerox (inviati a Xerox Services Manager).
Identità Device Management	Include le informazioni del PC host dell'applicazione come il nome DNS, l'indirizzo IP, il nome del sistema operativo, il tipo di sistema operativo, la CPU del PC, le dimensioni della RAM (libera vs. usata), le dimensioni del disco rigido (libero vs. usato), il nome del sito, la versione dell'app, la data di scadenza della licenza dell'app, la versione .Net, il fuso orario, la versione del componente di individuazione, la dimensione del database principale, la dimensione del database di individuazione, il numero di stampanti/ in ambito/fuori ambito, i servizi critici in esecuzione.
Modalità di sicurezza aziendale Device Manager	Modalità normale = Xerox Device Agent contatta Xerox Services Manager, Daily. Le impostazioni possono essere modificate da remoto senza la necessità di visite in loco, anche quando i programmi di polling sono disattivati. Modalità di blocco = Oltre alla sincronizzazione dei dati relativi alla stampante, non vi è alcuna comunicazione con Xerox Services Manager e le impostazioni devono essere modificate in loco. La macchina Xerox Device Agent e gli indirizzi IP della stampante vengono segnalati a Xerox Services Manager.

Attributi dei dati	Descrizione dettagliata degli attributi dei dati
Politica di controllo delle stampe Device Management	Include il nome del PC dell'utente finale, il server di stampa utilizzato, la coda di stampa utilizzata, l'indicatore ora della violazione, il nome del documento, il nome utente dell'utente finale, il duplex del lavoro, il colore del lavoro, le impressioni totali del lavoro, il prezzo del lavoro, l'azione eseguita, la notifica dell'utente finale, il messaggio visualizzato, il nome del criterio di stampa, la regola del criterio di stampa.

6. Gestione remota dei dispositivi di stampa

Il personale di supporto Xerox può elaborare le seguenti azioni tramite l'applicazione Device Direct o Xerox Device Management.

La Tabella 4 mostra gli sforzi di risoluzione migliorati, consentiti dal cliente in uno scenario di supporto intensificato. L'autorizzazione da parte del cliente a svolgere queste funzioni deve essere esplicitamente ottenuta.

Dati	Descrizione
Azioni da eseguire sui dispositivi di stampa	• Ottieni stato dispositivo = recupera lo stato più recente del dispositivo di stampa • Riavvia dispositivo = avvia una sequenza di spegnimento/accensione sul dispositivo di stampa • Aggiorna dispositivo = installa nuovi software/firmware sul dispositivo di stampa (.DLM sulla porta 9100) • Analisi problemi dispositivo = ping del dispositivo + recupera l'ultimo stato dal dispositivo di stampa • Stampa pagina di prova = invia un lavoro di prova a un dispositivo di stampa per convalidare il percorso di stampa (genera un report di configurazione) • Avvia gestione del dispositivo = avvia trasferimenti periodici di dati del dispositivo di stampa ai server di comunicazione Xerox® esterni **Nota: Ogni azione può essere disabilitata per l'utilizzo on-demand all'interno della parte di configurazione amministrativa delle applicazioni Xerox® Device Management che supportano questa funzione.**
Azioni da eseguire sulle Applicazioni Device Management	Le impostazioni all'interno di ciascuna applicazione di gestione dei dispositivi che possono essere gestite includono il funzionamento di rilevamento, la frequenza di esportazione dei dati, le impostazioni relative alla comunicazione SNMP (riprova, timeout, nomi della community), i profili di avviso e la frequenza di aggiornamento del software dell'applicazione di gestione automatica dei dispositivi.

Dati	Descrizione
Gestione remota del software	Alcuni dispositivi sono dotati di funzionalità automatizzate di gestione remota del software. Questi dispositivi inviano una query all'ambiente Xerox per verificare se sono disponibili nuovi aggiornamenti software per il dispositivo. Se presenti, il dispositivo sarà in grado di inviare una richiesta per tale aggiornamento software e sarà aggiornato al momento prescritto. Tuttavia, se l'ambiente in uso vieta gli aggiornamenti automatici del software, l'opzione di gestione del software remoto può essere deselezionata solo senza interrompere i servizi remoti standard.

Requisiti di sistema per le Applicazioni Device Management

I requisiti minimi variano leggermente a seconda delle offerte. Consultare la Guida per l'utente, la Guida alla valutazione della sicurezza e/o la Guida alla certificazione per i requisiti di base specifici per le rispettive applicazioni di gestione dei dispositivi.

Al momento dell'installazione, viene incluso un file .readme per soddisfare i requisiti di sistema aggiuntivi e specifici per la rispettiva applicazione di gestione del dispositivo in fase di installazione.

- Le applicazioni Device Management sono compatibili con le funzionalità di sicurezza integrate nel sistema operativo Windows®. Si basano su un servizio Windows® in background in esecuzione con le credenziali dell'account di sistema locale per consentire il monitoraggio proattivo delle stampanti e il payload dell'attributo dei dati di stampa che verrà trasmesso a Xerox. L'interfaccia utente che visualizza il payload dell'attributo dei dati di stampa è accessibile solo da utenti esperti e amministratori con accesso al sistema operativo Windows®.

- Per evitare un'interruzione delle comunicazioni automatiche dei servizi remoti, si consiglia di caricare l'applicazione Device Management su un client alimentato in modo continuo o durante l'orario di lavoro principale.

- È consigliabile che i computer host eseguano un sistema operativo supportato da Microsoft® Corporation. Tuttavia, le applicazioni Xerox Device Management possono essere eseguite su Apple® OS 10.9.4 o versioni successive utilizzando il software di emulazione Parallels Desktop. L'applicazione non verrà eseguita nell'ambiente Macintosh nativo. Consultare le rispettive guide utente per il supporto dettagliato. È possibile trovare i requisiti per l'esecuzione su un sistema operativo Macintosh

- È consigliabile che i computer host siano aggiornati con le patch critiche e le release di servizio più recenti di Microsoft® Corporation.

- È necessario che il TCP/IP (Network Transmission Control Protocol/Internet Protocol) sia caricato e operativo.

- Per installare il software dell'applicazione Device Management sulla macchina client sono necessari privilegi amministrativi.

- Richiede dispositivi abilitati per SNMP e la possibilità di instradare SNMP sulla rete. Non è necessario abilitare SNMP nel computer in cui verranno installate le applicazioni Xerox® Device Management o in qualsiasi altro computer di rete.

- Prima di installare l'applicazione, è necessario installare Microsoft®.NET Framework.

- L'applicazione non deve essere installata su un PC in cui sono installate altre applicazioni basate su SNMP o altri strumenti di gestione Xerox® Print, in quanto potrebbero interferire con il funzionamento reciproco.

Configurazioni del database

- L'applicazione installa il motore di database SQL Server Compact Edition (SQL CE) e i file di database che memorizzano i dati della stampante e le impostazioni dell'applicazione nella directory di installazione. Non è necessaria alcuna licenza di database per l'applicazione. Xerox® Device Agent supporta inoltre le istanze esistenti di SQL Server, come descritto in precedenza.

Configurazioni non supportate

In questa sezione vengono descritte le configurazioni non supportate.

- Installazione dell'applicazione su un computer con un'altra applicazione di gestione del dispositivo Xerox, ad esempio Xerox Device Manager.

- Software nativo del sistema operativo Mac OS® (ad esempio, Xerox Device Agent può essere eseguito solo sulla piattaforma Apple Mac quando è installato il software di emulazione Parallels).

- Qualsiasi versione di sistemi operativi UNIX®, sistemi operativi Linux®, sistemi Windows® che eseguono il client Novell, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 e 2008 R2, Windows® Server 2003, Windows® 8 RT, sistemi operativi che eseguono Servizi terminal per applicazioni e installazione su sistemi Windows che eseguono controller di dominio.

Poiché questa applicazione è stata testata solo sull'ambiente VMware® Lab Manager/workstation, non sono supportati altri ambienti virtuali.

7. Processi e servizi aziendali Xerox®

I dati ricevuti dai dispositivi di stampa basati su Xerox® Office, dai dispositivi di stampa basati su Xerox® Production e dalle applicazioni Xerox Device Management come parte della soluzione di servizi remoti vengono utilizzati dai processi aziendali Xerox elencati di seguito:

La tabella 5 riporta in dettaglio il nome e la descrizione del processo aziendale e dei servizi supportati come parte della soluzione Servizi remoti.

Nome dei processi di business	Descrizione
Letture contatore automatico	I dati di lettura del contatore vengono utilizzati nel processo di fatturazione.
Rifornimento forniture automatico/Rifornimento parti automatico	Il toner viene inviato automaticamente ai clienti in base allo stato di esaurimento del materiale di consumo ricevuto dai dispositivi di stampa. Alcuni componenti sostituibili vengono spediti automaticamente ai clienti quando necessario per i loro dispositivi di stampa. Queste opzioni sono disponibili solo per i clienti che optano per contratti di fornitura a consumo.
Manutenzione (Assistente alla manutenzione)	La gestione remota del dispositivo fornisce informazioni dettagliate sui guasti che possono essere visualizzate dal personale di assistenza Xerox, quando necessario, per accelerare la preparazione per una visita in loco o diagnosticare e risolvere i problemi.
Supporto di 3° livello (Ingegneria/Debug)	Il personale di supporto del prodotto può eseguire il debug di problemi difficili quando ha accesso a registri di progettazione e debug dettagliati.
Sviluppo del prodotto	Le prestazioni della stampante e i dati di utilizzo vengono utilizzati per identificare i miglioramenti del prodotto per le versioni future.

I dati di base del dispositivo di stampa vengono aggregati, trasmessi, conservati e archiviati all'interno di un data center Xerox certificato ISO-27001 e conservati in conformità con le politiche di conservazione della gestione dei dati aziendali Xerox.

I processi e le pratiche di lavoro che supportano e proteggono i sistemi software dei servizi remoti si basano sulle migliori pratiche ITIL e sulle politiche di sicurezza delle informazioni Xerox che si allineano direttamente agli standard del sistema di gestione della sicurezza delle informazioni ISO 27002 dell'Organizzazione internazionale degli standard. I clienti possono essere certi che la gestione, la protezione e l'archiviazione dei dati del dispositivo comprendano i principi di base della sicurezza delle informazioni: riservatezza, integrità, disponibilità, autenticazione e non rifiuto.

8. Dettagli tecnologici

Questa sezione fornisce ulteriori dettagli tecnici che sono tipicamente richiesti dai team di Information Technology (IT) e dagli operatori della sicurezza che gestiscono i rischi, ottenendo la garanzia di pratiche di sviluppo sicure. Tale garanzia consente loro di certificare i nostri dispositivi di stampa e le applicazioni di gestione dei dispositivi per l'utilizzo nell'ambiente di rete del cliente.

Progettazione software

Il nostro impegno per la sicurezza dei prodotti Xerox comincia all'inizio dello sviluppo dei prodotti, durante il quale gli sviluppatori Xerox seguono un ciclo di vita formale di sviluppo della sicurezza che gestisce i problemi di sicurezza attraverso l'identificazione, l'analisi, la definizione delle priorità, la codifica e il test. Molti dispositivi di stampa Xerox® sono certificati Common Criteria ISO IEC 15408 o sono attivamente in fase di revisione della certificazione.

Operatività

I servizi remoti Xerox eseguono i seguenti tipi di operazioni su una rete. Queste operazioni dipendono dal metodo di distribuzione configurato.

Tabella 6.

Metodo implementazione	Applicazione usata	Flusso di dati sulla rete	Operatività imposta su una rete
Device Direct	Nessuno	Interno	Il dispositivo di stampa Xerox® tenta di rilevare un Server proxy web (automatico o indirizzato a un indirizzo specifico)
		Interno	I dispositivi di stampa Xerox® possono essere programmati per generare richieste a un server SMTP (Simple Mail Transport Protocol) per inviare per inviare messaggi email con notifiche di avviso a un elenco di destinatari predefinito
		Esterno alla rete	Il dispositivo di stampa Xerox® attraversa il firewall aziendale per accedere a Internet (HTTPS sulla porta 443)
		Esterno alla rete	Il dispositivo di stampa Xerox® esegue l'autenticazione con il proprio certificato al server di comunicazione Xerox remoto prima di trasmettere qualsiasi attributo di dati
		Esterno alla rete	Il dispositivo di stampa Xerox® trasmette automaticamente i dati degli attributi del dispositivo di stampa attraverso un canale crittografato (HTTPS sulla porta 443) ai server di comunicazione Xerox® a un'ora specificata quotidianamente o su richiesta del cliente.
		Esterno alla rete	Il dispositivo di stampa Xerox® interroga automaticamente i server di comunicazione Xerox® attraverso un canale crittografato (HTTPS sulla porta 443) a un'ora specifica ogni giorno per ottenere un elenco di azioni da eseguire (ad esempio inviare ora i dati di fatturazione, aggiungere un servizio, ecc.)

Metodo implementazione	Applicazione usata	Flusso di dati sulla rete	Operatività imposta su una rete
		Esterno alla rete	Trasmissione unidirezionale on-demand dei dati del registro tecnico del dispositivo Xerox® Print attraverso un canale crittografato (HTTPS sulla porta 443) a Xerox® Communication Server
Device Direct	Nessuno	In uscita, avviato dallo sviluppatore per tirare l'ultimo s/w	Il dispositivo invia una query al server di gestione software remoto per verificare la presenza di aggiornamenti software/di sicurezza. Tuttavia, se l'ambiente in uso vieta gli aggiornamenti automatici del software, l'opzione di gestione del software remoto può essere deselezionata solo senza interrompere i servizi remoti standard.
Applicazioni Device Management	Centre Ware® Web	Interno	Ogni applicazione rileva un server proxy Web (automatico o indirizzato a un indirizzo specifico)
		Interno	Ogni applicazione recupera le funzionalità del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione recupera la configurazione del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione recupera lo stato del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione recupera i dati di consumo del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione può riavviare un dispositivo di stampa tramite SNMP o tramite l'interfaccia utente web del dispositivo di stampa
		Interno	Ogni applicazione può inviare una pagina di prova a un dispositivo di stampa specifico
		Interno	Ogni applicazione può avviare la pagina web di un dispositivo di stampa
		Esterno **(solo in uscita)**	Ogni applicazione attraversa il firewall aziendale per accedere a Internet (HTTPS sulla porta 443)
		Esterno (**solo in uscita)**	Ciascuna app esegue l'autenticazione con il suo certificato sul server di comunicazione Xerox remoto prima di trasmettere qualsiasi attributo dei dati
		Esterno **(solo in uscita)**	Ogni applicazione trasmette automaticamente i dati degli attributi del dispositivo di stampa attraverso un canale crittografato (HTTPS sulla porta 443) ai server di comunicazione Xerox® a un'ora specifica ogni giorno
		Esterno **(solo in uscita)**	Ogni applicazione interroga automaticamente i server di comunicazione Xerox® attraverso un canale crittografato (HTTPS sulla porta 443) a un'ora specifica ogni giorno per un elenco di azioni da eseguire
		Interno	Ogni applicazione Xerox Device Agent rileva un server proxy Web (automatico o indirizzato a un indirizzo specifico)

Metodo implementazione	Applicazione usata	Flusso di dati sulla rete	Operatività imposta su una rete
Applicazioni Device Management	Xerox	Interno	Ogni applicazione Xerox Device Agent recupera le funzionalità del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione Xero® Device Agent recupera la configurazione del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione Xerox Device Agent recupera lo stato del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione Xerox Device Agent recupera i dati di consumo del dispositivo di stampa attraverso la flotta tramite SNMP
		Interno	Ogni applicazione Xerox Device Agent può richiedere che il dispositivo stampi un report di configurazione
		Interno	Ogni applicazione Xerox Device Agent può avviare la pagina Web di un dispositivo di stampa
		Interno	Ogni applicazione Xerox Device Agent può aggiornare il software del dispositivo di stampa tramite l'invio del lavoro di stampa. (. File DLM sulla porta 9100)
		Esterno (**solo in uscita)**	Ogni applicazione Xerox Device Agent attraversa il firewall aziendale per accedere a Internet (HTTPS sulla porta 443)
		Esterno (**solo in uscita)**	Ciascuna app esegue l'autenticazione con il suo certificato sul server di comunicazione Xerox remoto prima di trasmettere qualsiasi attributo dei dati
		Esterno **(solo in uscita)**	Ogni applicazione Xerox Device Agent trasmette automaticamente i dati degli attributi del dispositivo di stampa attraverso un canale crittografato (HTTPS sulla porta 443) ai server di comunicazione Xerox® a un'ora specifica ogni giorno
		Esterno **(solo in uscita)**	Ciascuna app Xerox Device Agent interroga automaticamente i server di comunicazione attraverso un canale crittografato (HTTPS sulla porta 443) a un'ora specifica ogni giorno per un elenco di azioni da eseguire
		Interno	Le app Xerox Device Manager/Xerox Device Agent rilevano un server proxy Web (automatico o indirizzato a un indirizzo specifico)
		Interno	Le app Xerox Device Manager/Xerox Device Agent recuperano le funzionalità dei dispositivi di stampa attraverso la flotta tramite SNMP
		Interno	Le app Xerox Device Manager/Xerox Device Agent recuperano la configurazione dei dispositivi di stampa attraverso la flotta tramite SNMP
		Interno	Le app Xerox Device Manager/Xerox Device Agent recuperano lo stato dei dispositivi di stampa attraverso la flotta tramite SNMP
		Interno	Le app Xerox Device Manager/Xerox Device Agent recuperano i materiali di consumo dei dispositivi di stampa attraverso la flotta tramite il protocollo SNMP
		Interno	Le app Xerox Device Manager/Xerox Device Agent possono richiedere che il dispositivo stampi un report di configurazione

Metodo implementazione	Applicazione usata	Flusso di dati sulla rete	Operatività imposta su una rete
Applicazioni Device Management	Xerox® Device Manager per il monitoraggio dei dispositivi di stampa connessi in rete	Interno	Le app Xerox Device Manager/Xerox Device Agent possono lanciare la pagina web di un dispositivo di stampa
		Interno	Le app Xerox Device Manager/Xerox Device Agent possono aggiornare il software del dispositivo di stampa tramite l'invio di un lavoro di stampa
		Interno	L'app Xerox Device Manager supporta le comunicazioni SNMPv3 con i dispositivi di stampa
		Interno	L'app Xerox Device Manager può apportare modifiche alla configurazione del dispositivo di stampa tramite il protocollo SNMP e l'interfaccia utente Web
		Interno	L'app Xerox Device Manager recupera i registri di contabilità basati sui lavori di stampa da alcuni sistemi multifunzione MFP Xerox®
		Interno	L'app Xerox Device Manager gestisce/impone le politiche di controllo delle stampe
		Esterno **(solo in uscita)**	Le app Xerox Device Manager/Xerox Device Agent attraversano il firewall aziendale per accedere a Internet (HTTPS sulla porta 443)
		Esterno (**solo in uscita)**	Ciascuna app esegue l'autenticazione con il suo certificato sul server di comunicazione Xerox remoto prima di trasmettere qualsiasi attributo dei dati
		Esterno **(solo in uscita)**	Le app Xerox Device Manager/Xerox Device Agent trasmettono automaticamente i dati del dispositivo di stampa ai server di comunicazione Xerox® tramite un canale crittografato (HTTPS sulla porta 443) a un'ora specifica ogni giorno
		Esterno **(solo in uscita)**	Le app Xerox Device Manager/Xerox Device Agent eseguono automaticamente query sui server di comunicazione Xerox attraverso un canale crittografato (HTTPS sulla porta 443) a un'orario specifico ogni giorno per un elenco di azioni da eseguire
	Applicazione Device Management	Esterno, bidirezionale	Xerox Device Manager contatta ogni giorno Xerox Services Manager e consente agli amministratori di modificare in remoto le impostazioni, evitando l'esigenza di chiamate di assistenza in loco.

9. Funzioni di protezione

SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) PER XEROX®

Il protocollo SNMP (Simple Network Management Protocol) è lo strumento di gestione della rete più utilizzato per la comunicazione tra i sistemi di gestione della rete e le stampanti in rete. Le applicazioni Device Management utilizzano SNMP durante le operazioni di individuazione per recuperare informazioni dettagliate sul dispositivo di stampa. Le applicazioni Xerox® Device Management supportano i protocolli SNMP v1/v2 e v3. Consultare le rispettive guide alla certificazione dell'applicazione Xerox® Device Management per dettagli specifici.

Il framework SNMP v3 supporta più modelli di sicurezza, che possono esistere contemporaneamente all'interno di un'entità SNMP. SNMPv3 include una maggiore protezione aggiungendo la protezione crittografica a SNMPv2. Inoltre, SNMPv3 è retrocompatibile con le versioni precedenti ed è ampiamente utilizzato in reti solide.

Le applicazioni Xerox Device Management (Centre Ware® Web/Xerox Device Manager, Xerox Device Agent) possono comunicare con piattaforme di dispositivi conformi allo standard FIPS 140-2 (Federal Information Processing Standard) nelle loro implementazioni di SNMPv3.

Le applicazioni Xerox Device Management non utilizzano il servizio SNMP di Windows o il servizio trap SNMP di Windows. Se installati in precedenza, questi servizi **devono** essere disabilitati su qualsiasi personal computer (PC) o server in cui è installata l'applicazione Xerox Device Management.

Le applicazioni Xerox Device Management utilizzano un agente SNMP sviluppato da Xerox che:

- Contiene uno speciale meccanismo di codifica/decodifica
- È completamente gestito da .NET
- Utilizza l'eseguibile runtime .NET, che offre una maggiore sicurezza per prevenire gli attacchi contro le vulnerabilità del software, quali manipolazioni di puntatori non validi, overrun di buffer e bound checking.

Le applicazioni Xerox Device Management utilizzano le funzioni di sicurezza disponibili nel sistema operativo Windows, tra cui:

- Autenticazione e autorizzazione degli accessi utente
- Configurazione e gestione dei servizi
- Distribuzione e gestione di criteri di protezione di gruppo

Firewall connessione Internet Windows (ICF), tra cui:

- Impostazioni registro di protezione
- Impostazioni ICMP

Applicazioni Xerox Device Management: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE application Microsoft® SQL Server e **Xerox Device Manager** utilizzano Microsoft® SQL Server.

Le applicazioni Xerox Device Management possono essere configurate in modo da sfruttare le funzionalità di sicurezza aggiuntive di Microsoft® in modo da includere, ove applicabile:

- Abilitazione della registrazione dell'account utente
- Crittografia del DNS (Domain Name System)
- Limite dei privilegi dell'account utente per accedere al database (ad esempio i diritti del proprietario del database)
- Implementazione di numeri di porta definiti dall'utente

Per trasmettere i dati ai server di comunicazione Xerox remoti sono necessari una chiave di registrazione Xerox e un account Xerox valido.

Le comunicazioni esterne delle applicazioni Xerox Device Management potrebbero essere influenzate da Windows Internet Connection Firewall. (È **consigliabile** che i clienti inseriscano l'URL Xerox nel firewall del cliente (* .support.xerox.com) e specifichino l'indirizzo IP che può accedere all'URL.)

Le applicazioni Xerox Device Management vengono eseguite come processo in background utilizzando le credenziali dell'account di sistema locale per interrogare automaticamente i dispositivi di stampa di rete tramite SNMP e trasmettere periodicamente gli attributi dei dispositivi di stampa ai server di comunicazione Xerox

L'accesso alle interfacce utente e alle funzionalità dell'applicazione Xerox Device Manager è controllato tramite i seguenti privilegi basati sui ruoli:

- Amministratori Web di Centre Ware®, Utenti Web Power di Centre Ware®, Utenti Web SQL di Centre Ware®, Amministratori clienti Web di Centre Ware® e Gruppi clienti Web di Centre Ware®.
- I nomi utente e le password per le applicazioni non attraversano la rete; vengono invece utilizzati i token di accesso (per design del sistema operativo Windows®).
- L'applicazione Xerox Device Manager offre una sicurezza basata sul controllo dell'invio delle stampe, limitando i lavori in base ai criteri di utilizzo del colore, al tipo di documento, al costo del lavoro, all'ora del giorno, al controllo dell'accesso dei gruppi di utenti, ai criteri duplex, alle stampe consentite e alle quote di stampa.

Nota: L'utilizzo di SNMP da parte di qualsiasi applicazione Xerox® Remote Services non rappresenta un rischio per la sicurezza dell'ambiente IT di un client, in quanto tutto il traffico basato su SNMP generato o consumato da queste applicazioni si verifica all'interno della rete Intranet del client, dietro il firewall. Il servizio SNMP di Windows e il servizio trap SNMP di Windows non sono abilitati nel sistema operativo Windows per impostazione predefinita.

Modalità di protezione aziendale

Per impostazione predefinita, la sincronizzazione ***pianificata*** dall'applicazione Xerox Device Agent con il server di comunicazione protetto viene impostata su *giornaliera*. Si noti che l'ora del giorno può essere impostata su un'ora prescelta.

Esistono due modalità di sicurezza aziendali: **Normal** e **Locked Down.**

Quando è impostata la modalità **Normal**, l'applicazione Device Management contatta Xerox Services Manager quotidianamente.Le impostazioni possono essere modificate senza la necessità di visite sul posto, anche quando i programmi di polling sono disattivati. ***(Modalità consigliata***).

In modalità **Locked Down**, oltre alla sincronizzazione dei dati relativi alla stampante, non vi è alcuna comunicazione con i server di comunicazione e le impostazioni devono essere modificate sul posto. Inoltre, il computer Xerox Device Agent e gli indirizzi IP della stampante non vengono segnalati al server di comunicazione. Questa modalità limita tutti gli altri vantaggi dei servizi remoti per includere la fatturazione e le forniture automatizzate, nonché i dati diagnostici utilizzati per il supporto tecnico.

Nota: Se una versione di Xerox Device Agent non contiene la scheda Modalità di protezione aziendale, funziona in modalità Normal.

10. Impatto sulla rete

Le linee guida di rete aziendali in genere abilitano o disabilitano porte di rete specifiche su router e/o server. La maggior parte dei reparti IT si preoccupa delle porte utilizzate dall'applicazione per il traffico in uscita. La disabilitazione di porte specifiche può influire sulla funzionalità dell'applicazione. Fare riferimento alla tabella seguente per le porte specifiche utilizzate dai processi dell'applicazione. Se l'applicazione deve eseguire la scansione su più segmenti di rete o sottoreti, i router devono consentire i protocolli associati a questi numeri di porta.

Protocolli, porte e altre tecnologie correlate

Tabella 7 Identifica i protocolli, le porte e le tecnologie utilizzate in Xerox® Remote Services:.

Numero porta	Protocollo	Descrizione dell'uso	Flusso dati sulla Rete
Dipende dai protocolli del livello superiore	**Internet Protocol (IP)**	**Trasporto sottostante per tutte le comunicazioni di dati**	**Interno + Esterno (solo in uscita)**
ND	Internet Control Message Protocol (ICMP)	Rilevamento e risoluzione dei problemi del dispositivo di stampa	Interno
25	Simple Mail Transport Protocol (SMTP)	Dispositivo di stampa + App proxy remota Avvisi di notifica e-mail	Interno
53	Domain Name Services (DNS)	Utilizzato per le operazioni di individuazione dei dispositivi di stampa basati su DNS	Interno
80	Hyper Text Transport Protocol (HTTP)	Stampa query pagina Web dispositivo + query pagina Web applicazione Device Management	Interno
135	Remote Procedure Call (RPC)	Rilevamento periferica di stampa	Interno
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Protocollo standard del settore utilizzato per individuare dispositivi di stampa in rete + Recuperare stato, contatori e fornire dati + Recuperare e applicare la configurazione della periferica di stampa. Nomi community predefiniti = “public” (GET), “private” (SET)	Interno

Numero porta	Protocollo	Descrizione dell'uso	Flusso dati sulla Rete
443	Hyper Text Transport Protocol Secure (HTTPS)	Stampa le query delle pagine Web protette del dispositivo (se configurate) + le query delle pagine Web protette dell'app Remote Proxy (se configurate) + Ritrasferimento dei dati del dispositivo di stampa ai server di comunicazione Xerox® + controllo delle comunicazioni di stampa a Xerox® Device Manager	Interno + Esterno (solo in uscita)
515, 9100, 2000, 2105	Invio lavoro di stampa LPR e porta raw TCP/IP	Aggiornamento software periferica di stampa + Diagnostica stampa pagina di prova	Interno

11. Best practice in materia di sicurezza

- Tenere sempre aggiornati i dispositivi di stampa con il firmware/software più recente. Xerox monitora attentamente le vulnerabilità e fornisce in modo proattivo ai clienti patch di sicurezza e aggiornamenti, quando necessario.
- Disabilitare le porte e i protocolli inutilizzati sui dispositivi di stampa ove possibile. Questa operazione viene in genere eseguita nell'interfaccia utente Web delle periferiche di stampa di classe Office e nell'interfaccia utente locale delle periferiche di stampa di classe Production.
- Utilizzare le funzioni relative al controllo degli accessi degli utenti sui dispositivi di stampa, se disponibili. Questa operazione viene in genere eseguita nell'interfaccia utente Web delle periferiche di stampa di classe Office e nell'interfaccia utente locale delle periferiche di stampa di classe Production.
- Utilizzare protocolli sicuri quando possibile. Questa operazione viene in genere eseguita nell'interfaccia utente Web delle periferiche di stampa per ufficio e nell'interfaccia utente locale delle periferiche di stampa per la produzione.
- Abilitare le funzionalità di sicurezza incorporate nel dispositivo (ad es. sovrascrittura delle immagini, crittografia dei dati di scansione, crittografia del flusso di stampa, crittografia del disco, stampa protetta, crittografia .pdf, autenticazione di accesso CAC/PIV).

Per ulteriori informazioni sui servizi remoti@ Xerox, visitare Xerox.com/RemoteServices.

Per ulteriori e specifiche informazioni relative ai meccanismi e alle funzionalità di sicurezza all'interno della gamma di applicazioni Xerox Device Management, consultare le rispettive guide:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Che si tratti di sicurezza dei dispositivi o dei contenuti, Xerox è all'avanguardia nella sicurezza proattiva per le odierne minacce emergenti. Visitare www.xerox.com/security per accedere a un'ampia gamma di informazioni sulla sicurezza, aggiornamenti, bollettini, white paper, patch e altro ancora.