



# Xerox<sup>®</sup> Remote Services

Documento sulla sicurezza

Versione 2,0  
Global Remote Services  
Gestione delle informazioni sulle  
tecnologie Xerox<sup>®</sup>

Gennaio 2017

BR19369

©2017 Xerox Corporation. Tutti i diritti riservati. Xerox® e Xerox con il marchio figurativo® sono marchi di Xerox Corporation negli Stati Uniti e/o in altri paesi.

Microsoft®, Windows®, Windows Vista®, SQL Server®, Microsoft®.NET, Windows Server®, Internet Explorer®, Access®, Windows Media Center e Windows NT® sono marchi o marchi registrati di Microsoft Corporation negli Stati Uniti e/o in altri paesi.

Apple®, Macintosh® e Mac OS® sono marchi registrati di Apple Inc.

McAfee® è un marchio registrato di McAfee Inc. o delle sue consociate negli Stati Uniti e in altri paesi.

ISO è un marchio registrato della International Organization for Standardization.

UNIX è un marchio registrato negli Stati Uniti e in altri paesi, concesso in licenza esclusivamente attraverso X/Open Company Ltd

Linux è un marchio registrato di Linus Torvalds.

Parallels Desktop è un marchio registrato di Parallels IP Holdings GmbH.

VMware® Lab Manager /Workstation /vSphere Hypervisor sono marchi registrati di VMware, INC. negli Stati Uniti e/o in altre giurisdizioni.

Questo documento è periodicamente soggetto a modifiche. Eventuali modifiche, imprecisioni tecniche ed errori tipografici verranno rettificati nelle edizioni successive.



IS 614672/IS 514590

Versione documento: 2.0 (Gennaio 2017).

# Sommario

<b>Obiettivi generali e destinatari</b> .....	<b>4</b>
<b>Remote Services</b> .....	<b>5</b>
Controlli del cliente.....	6
<b>Modelli di distribuzione</b> .....	<b>7</b>
Modello di distribuzione Device Direct .....	8
Modello di distribuzione Applicazioni di gestione dei dispositivi .....	9
Modello di distribuzione misto .....	10
<b>Trasmissione dati e payload</b> .....	<b>11</b>
Fonti di dati .....	11
Dispositivi per ufficio Xerox® .....	11
Dispositivi di produzione Xerox® .....	13
Applicazioni di gestione dei dispositivi Xerox® .....	14
Gestione in remoto dei dispositivi di stampa .....	16
Requisiti di sistema per le applicazioni di gestione dei dispositivi .....	17
Configurazioni non supportate .....	17
Processi aziendali Xerox® e servizi .....	18
<b>Dettagli tecnici</b> .....	<b>19</b>
Progettazione del software.....	19
Operabilità .....	19
SNMP (Simple Network Management Protocol).....	23
Modalità di protezione aziendale .....	24
Protocolli, porte e altre tecnologie correlate.....	25
Procedure consigliate relative alla sicurezza.....	27

# Obiettivi generali e destinatari

Lo scopo del presente documento è di fornire una guida alla distribuzione di Xerox® Remote Services per stampanti Xerox e non Xerox in rete nell'ambiente del cliente. Il documento è destinato a fornire i dettagli relativi alla sicurezza e alla comprensione delle ampie misure di sicurezza implementate in Xerox® Remote Services.

I destinatari del documento sono fornitori di tecnologia, responsabili di reti IT e professionisti della sicurezza IT interessati alle funzionalità di Remote Services e all'implementazione della sicurezza di tali funzioni.

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

# Remote Services

Le informazioni rappresentano una risorsa chiave, e la sicurezza è fondamentale per tutte le risorse aziendali, inclusi i sistemi multifunzione collegati in rete. Nell'odierno mondo dell'"all-in-one", la gestione di un parco di sistemi multifunzione e al contempo il garantire un livello accettabile di sicurezza presenta una serie di problematiche uniche nel loro genere, che spesso vengono trascurate. Xerox® comprende tale complessità ed è pronta a rispondere alle esigenze di sicurezza dei clienti. I prodotti, i sistemi e la gamma di servizi remoti Xerox® sono progettati per essere integrati in modo sicuro nei flussi di lavoro esistenti dei nostri clienti, e adottare al contempo le più avanzate tecnologie protette.

Il Documento sulla sicurezza di Xerox® Remote Services intende aiutare i clienti a comprendere e distribuire la soluzione Remote Services sicura appropriata che sia compatibile con la loro infrastruttura di rete. La tipologia di rete del cliente stabilirà se sia necessario apportare modifiche al firewall, ai server proxy web o ad altre infrastrutture di rete relative alla sicurezza. La soluzione Xerox® Remote Services, il dispositivo e i controlli scelti dipendono dalle politiche sulla sicurezza delle informazioni (IS) del cliente e determinano la modalità operativa utilizzata.

La funzionalità Xerox® Remote Services è disponibile in determinati modelli di apparecchiature. Questa funzionalità consente di gestire e assistere da remoto i dispositivi di stampa utilizzando i dati degli attributi dei dispositivi, che sono: **identità del dispositivo di stampa, proprietà, stato, livelli dei materiali di consumo, dati sull'utilizzo e dati diagnostici dettagliati del dispositivo di stampa**. I dati degli attributi del dispositivo di stampa vengono trasmessi dall'interno dell'ambiente in rete del cliente direttamente dal dispositivo di stampa (funzionalità "device direct"), attraverso un'applicazione in hosting (applicazione di gestione del dispositivo), o attraverso una combinazione di entrambi i metodi utilizzando il percorso di comunicazione protetto di Xerox® Remote Services. Sia i dispositivi Xerox® che le applicazioni di gestione dei dispositivi Xerox® dispongono di un certificato per autenticarsi con i server di comunicazione Xerox® prima che possa essere eseguita la trasmissione degli attributi di stampa. Le transazioni di Xerox® Remote Services hanno origine sempre all'interno dell'ambiente del cliente e vengono inviate rigorosamente in base alle autorizzazioni del cliente.

I server di comunicazione Xerox® situati negli Stati Uniti sono conformi ai rigorosi requisiti di sicurezza per la gestione della sicurezza delle informazioni. I centri dati Xerox® e l'applicazione Xerox® Remote Services soddisfano i requisiti di conformità allo Statement on Standards for Attestation (SSAE) No-16, Sarbanes-Oxley Act (SOX) e sono certificati ISO 27001:2013.

**Per impostazione predefinita, non vengono trasmesse immagini del cliente provenienti da operazioni di stampa, fax, scansione e copia, né informazioni riservate, ai server di comunicazione Xerox®.**

## Controlli del cliente

Le applicazioni di gestione dei dispositivi Xerox® hanno la capacità di visualizzare i registri di dati degli attributi dei dispositivi di stampa esportati a scopi di revisione e di verifica prima della crittografia e della trasmissione ai server di comunicazione remoti Xerox®. Per i dati dettagliati, consultare la rispettiva guida per l'utente dell'applicazione di gestione dei dispositivi Xerox®.

Alcuni dispositivi di stampa per uffici di piccole e medie dimensioni sono dotati di una funzione che consente ai clienti di scaricare e visualizzare i dati degli attributi del dispositivo di stampa prima che vengano crittografati e trasmessi ai server di comunicazione Xerox® remoti tramite il metodo di abilitazione Device Direct. Per verificare che uno specifico dispositivo di stampa disponga di questa funzionalità, accedere alla pagina Centroware Internet Services del dispositivo di stampa, scheda Stato, collegamento Smart eSolutions (o Remote Services), sotto la scheda Assistente alla manutenzione.

La soluzione Xerox® Remote Services può essere adattata su misura per conformarsi a politiche IS dei clienti che sottopongano a limitazioni o restrizioni rigorose determinati tipi di attributi dei dispositivi di stampa che possono essere trasmessi al di fuori della rete (ad esempio attributi relativi agli indirizzi di rete). Gli strumenti applicativi di gestione dei documenti Xerox® hanno la capacità di disattivare determinati campi dalla trasmissione.

I clienti hanno anche la possibilità di richiamare una *richiesta di eccezione* durante le trattative contrattuali per **“annullare la sottoscrizione”** (opt-out) alla soluzione Remote Services. Questa opzione impedisce qualsiasi comunicazione e funzionalità di supporto remoto di Remote Services per i dispositivi di stampa nell'ambito dell'account in questione.

Per facilitare le attività di supporto remoto di livello superiore, i clienti possono, se necessario, attivare la funzione di accesso remoto per ricevere versioni del software del dispositivo di stampa, patch di sicurezza, nonché sottoporre a diagnosi, riparare o modificare in remoto le configurazioni dei dispositivi di stampa al fine di correggere eventuali malfunzionamenti diagnosticati. L'accesso remoto non consente a Xerox® di visualizzare né di scaricare documenti, dati o altre informazioni del cliente contenuti o in transito sul dispositivo di stampa o nei sistemi informatici del cliente. Sussiste tuttavia un'eccezione a questa regola, che si verifica quando un cliente sta lavorando con personale di supporto Xerox su un problema di particolare difficoltà e viene stabilito che potrebbero essere necessarie ulteriori informazioni per risolvere il problema. In questa circostanza, un cliente potrebbe decidere di fornire a Xerox l'autorizzazione ad accedere ai registri archiviati localmente sul dispositivo e che contengono dati riservati.

Pertanto, i team IT (Information Technology) aziendali e i professionisti del settore della sicurezza sono invitati a leggere questo documento nella sua interezza al fine di comprendere a fondo le varie funzioni, i requisiti e le attività operative di Xerox® Remote Services e in che modo questa soluzione supporta la conformità alle politiche IS dei nostri clienti.

Risorse aggiuntive relative alla sicurezza per le protezioni dei dati di sicurezza dei prodotti Xerox®, le partnership del settore e le certificazioni sono disponibili all'indirizzo <http://www.xerox.com/security>.

# Modelli di distribuzione

I clienti possono scegliere tra i seguenti modelli di distribuzione di Xerox® Remote Services, che offrono lo stesso livello di protezione:

- **Modello Device Direct:** Device Direct consente ai dispositivi di stampa di comunicare direttamente con i server di comunicazione Xerox® remoti su Internet attraverso il firewall del cliente.
- **Modello Applicazioni di gestione dei dispositivi:** un'applicazione di gestione dei dispositivi Xerox® (chiamata Device Manager) può essere distribuita su una rete di un cliente per raccogliere un sottoinsieme di attributi di dati dai dispositivi di stampa. Gli attributi di più dispositivi di stampa vengono raccolti e quindi trasmessi in modo protetto ai server di comunicazione Xerox® remoti.
- **Modello misto:** l'implementazione sia del modello Device Direct che del modello Applicazioni di gestione dei dispositivi.

Tutti i modelli di distribuzione per Xerox® Remote Services sfruttano protocolli e porte standard del settore basati sul web per stabilire un canale protetto e crittografato per trasmettere gli attributi dei dispositivi di stampa esternamente ai server di comunicazione Xerox® situati nei centri dati protetti e ridondanti Xerox®.

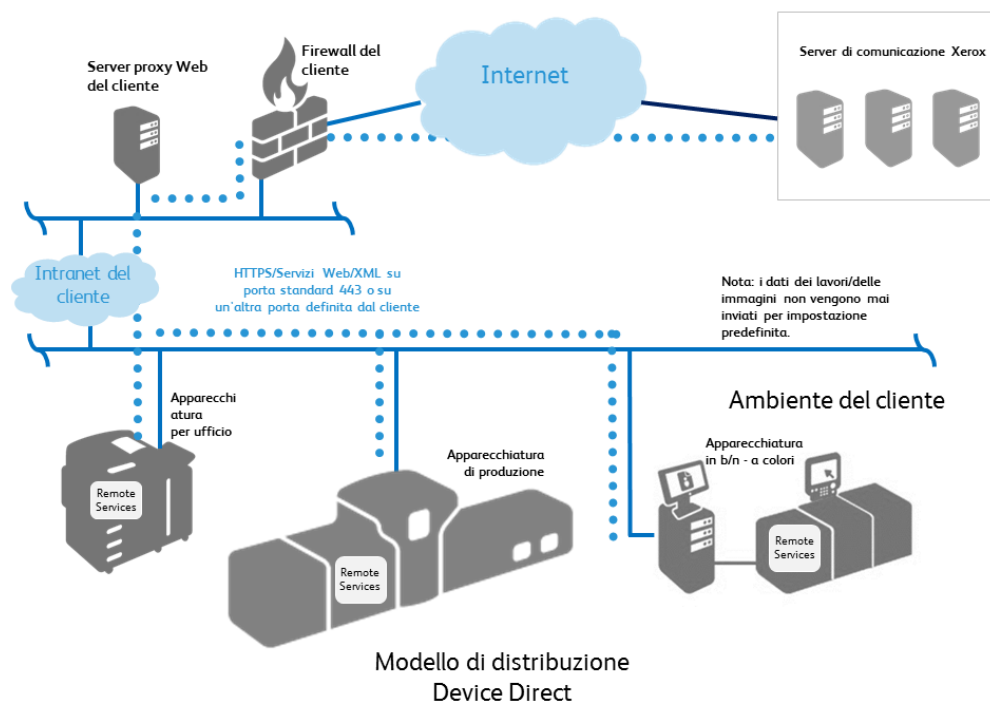
Il modello di distribuzione scelto dipende dalle politiche IS dei nostri clienti e dalle regole di gestione della trasmissione degli attributi dei dispositivi di stampa, nonché dal tipo di soluzione di servizi di stampa acquistata da Xerox® (servizi di stampa di base o gestiti).

# Modello di distribuzione Device Direct

Il modulo per servizi remoti incorporato con i dispositivi Xerox® utilizza una connessione TLS (Transport Layer Security) 1.2 sulla porta standard 443 per comunicare esternamente con i server di comunicazione Xerox® remoti.

- I dispositivi di stampa all'interno dell'ambiente del cliente avviano direttamente tutte le comunicazioni con i server di comunicazione Xerox® remoti. Per abilitare la comunicazione sono richieste configurazioni standard dei firewall presso la sede del cliente.
- Deve essere utilizzato un URL valido per i server di comunicazione Xerox® remoti.
- I server di comunicazione Xerox® si trovano dietro un firewall protetto e non sono accessibili da Internet.

Figura 1



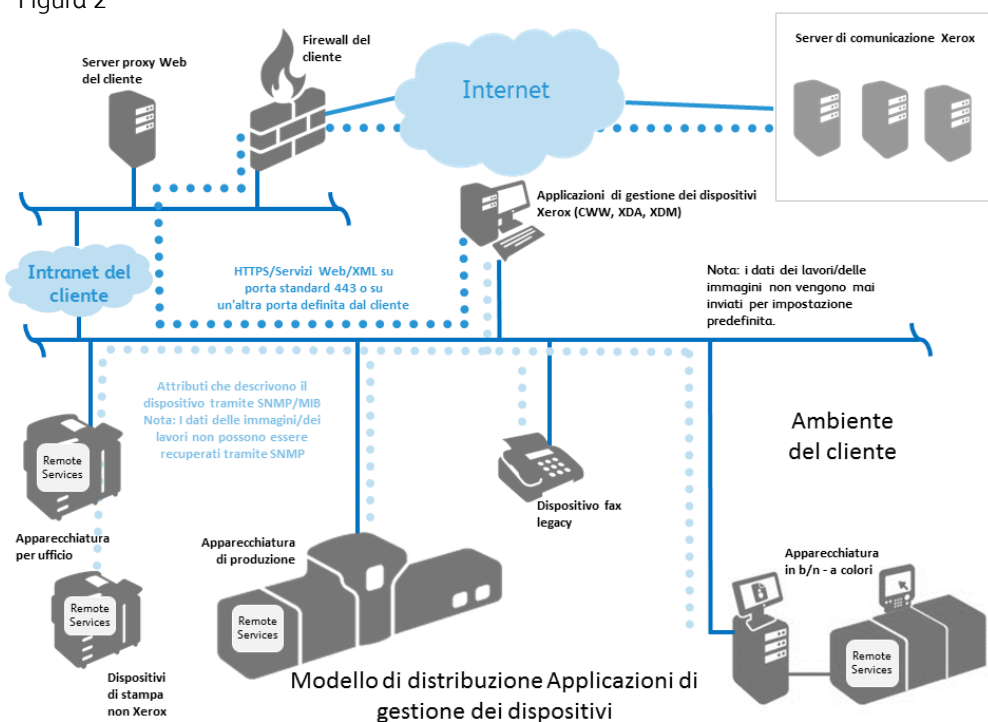


# Modello di distribuzione Applicazioni di gestione dei dispositivi

Anche le applicazioni di gestione dei dispositivi (vale a dire **Xerox® Centre Ware® Web**, **Xerox® Device Agent**, **Xerox® Device Agent Partner Edition**, e **Xerox® Device Manager**) utilizzando una connessione crittografata protetta TLS (Transport Layer Security) 1.2 sulla porta standard 443 per poter comunicare esternamente con i server di comunicazione Xerox® remoti. Per incrementare la sicurezza attraverso questo canale, vengono sfruttate funzioni aggiuntive che vengono stabilite durante l'installazione iniziale delle applicazioni di gestione dei dispositivi, che includono quanto segue:

- L'applicazione di gestione dei dispositivi all'interno dell'ambiente del cliente avvia tutte le comunicazioni con i server di comunicazione Xerox® remoti. Per abilitare la comunicazione sono richieste configurazioni standard dei firewall presso la sede del cliente.
- Deve essere utilizzato un URL valido per i server di comunicazione Xerox® remoti.
- I server di comunicazione Xerox® si trovano dietro un firewall protetto e non sono accessibili da Internet.
- È necessario utilizzare un ID account valido o un identificatore del sito e un codice di registrazione del server di comunicazione Xerox® per poter accedere ad alcuni dei servizi dei server di comunicazione Xerox®.
- L'applicazione di gestione dei dispositivi richiede una registrazione ai server di comunicazione Xerox® remoti utilizzando le credenziali appropriate di autenticazione del certificato.
- I server di comunicazione Xerox® remoti convalidano le credenziali fornite e accettano le richieste.
- L'applicazione di gestione dei dispositivi autentica i server di comunicazione Xerox® remoti e attiva il servizio.

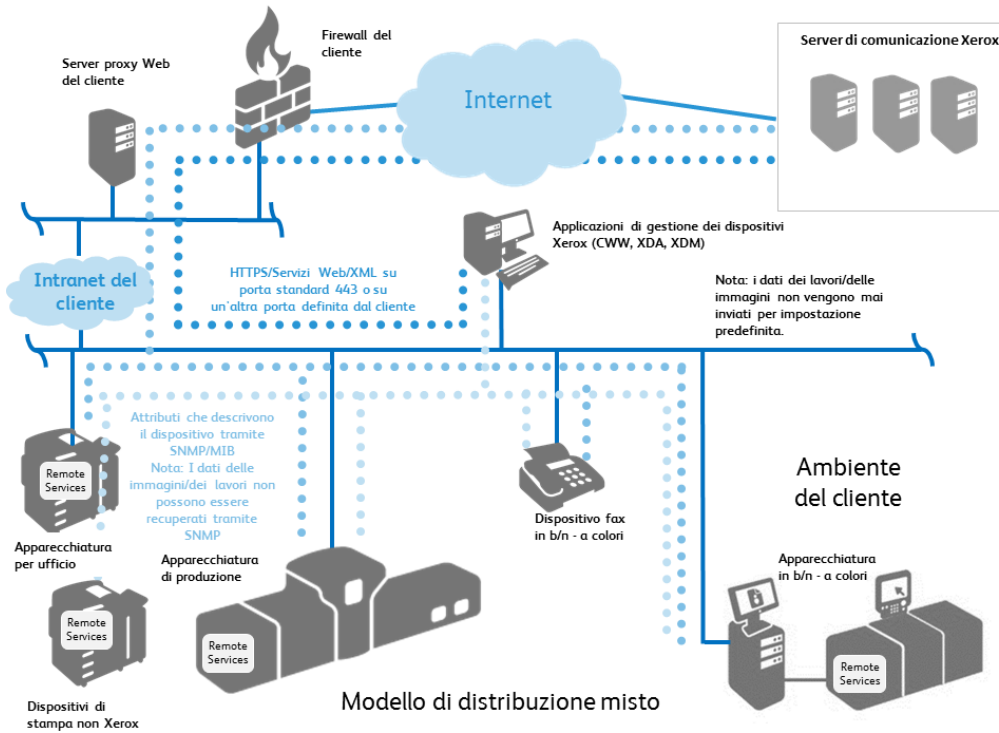
Figura 2



# Modello di distribuzione misto

La distribuzione mista viene eseguita ogni volta che un cliente acquista diversi tipi di contratti di manutenzione Xerox per i propri dispositivi di stampa. Quando un dispositivo di stampa Xerox® viene inizialmente installato in una rete, l'impostazione predefinita di Xerox® Remote Services fa sì che il dispositivo di stampa tenti automaticamente di stabilire una connessione diretta con i server di comunicazione Xerox®.

Figura 3



# Trasmissione dati e payload

## Fonti di dati

Gli attributi dei dati dei dispositivi di stampa vengono raccolti per Xerox® Remote Services dalle fonti seguenti:

- Stampanti di rete per ufficio Xerox®
- Stampanti di rete non Xerox®
- Stampanti di produzione Xerox®
- Applicazioni di gestione dei dispositivi Xerox®

## Dispositivi per ufficio Xerox®

I dispositivi di stampa Xerox® della categoria ufficio trasmettono gli attributi dei dati dei dispositivi in un formato XML (eXtensible Markup Language) utilizzando un file .zip compresso. Ciascun file viene quindi trasmesso attraverso un canale crittografato ai server di comunicazione remoti Xerox®.

La **Tabella 1** identifica l'attributo dei dati del dispositivo che può essere trasmesso e la relativa descrizione.

Attributi dati	Descrizione
<b>Identità del dispositivo di stampa</b>	Include modello, versione del firmware, numeri di serie del modulo e data di installazione.
<b>Indirizzo di rete del dispositivo di stampa</b>	Comprende indirizzo MAC (Media Access Control), indirizzo subnet.
<b>Proprietà del dispositivo di stampa</b>	Include una configurazione dettagliata dei componenti hardware, una configurazione dettagliata dei moduli software, le funzionalità/i servizi supportati, i modi di risparmio di energia, ecc.
<b>Stato del dispositivo di stampa</b>	Include lo stato generale, gli avvisi dettagliati, la cronologia degli ultimi 40 errori, i dati in inceppamento carta, ecc.
<b>Contatori del dispositivo di stampa</b>	Include parametri di fatturazione, contatori di stampa, di copie, di fax, di lavori di stampa di grandi dimensioni, di scansione diretta a destinazione, statistiche di utilizzo, ecc.
<b>Materiali di consumo del dispositivo di stampa</b>	Include il nome dei materiali di consumo, tipo (es: imaging, finitura, supporto carta), livello, capacità, stato, formato, ecc.

Attributi dati	Descrizione
<b>Utilizzo dettagliato del dispositivo di stampa</b>	Include contatori di stampa dettagliati, stati di alimentazione attivi, quantità dettagliate di sostituzione delle CRU (Customer Replaceable Unit), dati dettagliati degli errori e distribuzione delle CRU, utilizzo integrato della funzionalità OCR (Optical Character Recognition), distribuzione dei volume di stampa, distribuzione dell'utilizzo dei vassoi carta, supporti installati, distribuzione dei tipi e delle dimensioni dei supporti, distribuzione della lunghezza dei documenti, numero di fascicoli, dati HFSI, dati NVM, distribuzione, conteggi dei pixel marcati, copertura area media per colore, errori/inceppamenti, contatori dettagliati di scansione.
<b>Progettazione/Debug</b>	Comprende informazioni dettagliate di debug che potrebbero includere dati al di fuori della serie di dati suelencati. Tali dati possono includere informazioni di identificazione personale quali nomi utente, indirizzi e-mail e dati dei lavori. Tali dati vengono inviati con il consenso esplicito del cliente e sono destinati esclusivamente all'utilizzo per il supporto di livello superiore.

**Nota:** il file e il contenuto dei dati identificati variano in base al modello del prodotto.

## Dispositivi di produzione Xerox®

I dispositivi di stampa Xerox® della categoria produzione trasmettono gli attributi dei dati dei dispositivi in un formato XML (eXtensible Markup Language) utilizzando un file .zip compresso. Ciascun file viene quindi trasmesso attraverso un canale crittografato ai server di comunicazione Xerox® remoti.

La **Tabella 2** identifica gli attributi dei dati del dispositivo che possono essere trasmessi e la relativa descrizione.

Attributi dati	Descrizione dettagliata
<b>Identità del dispositivo di stampa</b>	Include modello, livelli di firmware dei moduli, numeri di serie dei moduli, date di installazione dei moduli, informazioni di contatto del cliente, dati relativi al contratto di licenza e posizione, se disponibile.
<b>Indirizzo di rete del dispositivo di stampa</b>	Comprende indirizzo MAC (Media Access Control), indirizzo subnet.
<b>Proprietà del dispositivo di stampa</b>	Include una configurazione dettagliata dei componenti hardware, una configurazione dettagliata dei moduli software, le funzionalità/i servizi supportati, ecc.
<b>Stato del dispositivo di stampa</b>	Include stati attivi, conteggi della cronologia degli errori, registro eventi, cronologia della trasmissione dati
<b>Contatori del dispositivo di stampa</b>	Include parametri di fatturazione, contatori di stampa, di copie, di lavori di stampa di grandi dimensioni, contatori specifici di produzione, di scansione a destinazione su modelli di fascia bassa, ecc.
<b>Materiali di consumo del dispositivo di stampa</b>	Include produttore, modello, numero di serie, nome, tipo, livello, capacità, stato, contatori della durata, ecc.
<b>Utilizzo dettagliato del dispositivo di stampa</b>	Include dati HFSI, dati NVM, sostituzione di parti, file registro DFE, dati di diagnosi dettagliati, risoluzione degli errori.
<b>Progettazione/ Debug</b>	Include dati dettagliati non strutturati relativi al debug concepiti esclusivamente per l'utilizzo del supporto di terzo livello.
<b>Cliente relativo al lavoro di stampa</b>	I dispositivi di stampa di produzione Xerox® offrono la capacità di riprodurre i dati relativi ai lavori a supporto degli scenari di assistenza di livello superiore, attraverso PostScript crittografato a Xerox. Il cliente può controllare se attivare o meno questa funzione. Se il cliente sceglie di ritrasmettere i dati relativi ai lavori (PostScript cifrato) a Xerox, tali dati vengono gestiti in base alle politiche IS e agli standard Xerox.

Esistono scenari di supporto di livello superiore, in cui sono previste informazioni dettagliate di debug che potrebbero includere attributi di dati al di fuori della serie di dati identificata nelle tabelle 1-3. Questi dati vengono inviati con il consenso esplicito del cliente e vengono gestiti in base alle politiche IS e agli standard protetti di Xerox.

**Nota:** il file e il contenuto dei dati identificati variano in base al modello del prodotto.

# Applicazioni di gestione dei dispositivi Xerox®

Le applicazioni di gestione dei dispositivi Xerox® (Xerox® Centre Ware® Web (CWW), Xerox® Device Agent (XDA), Xerox Device Agent Partner Edition (XDA PE) e Xerox® Device Manager (XDM) trasmettono i dati degli attributi di stampa in formato XML (eXtensible Markup Language) utilizzando un file .zip compresso. Il file viene quindi crittografato e trasmesso attraverso canali cifrati ai server di comunicazione Xerox® remoti.

La **Tabella 3** identifica gli attributi dei dati dei dispositivi e la relativa descrizione che possono essere inviati attraverso l'applicazione di gestione dei dispositivi Xerox®.

Attributi dati	Descrizione dettagliata
<b>Identità del dispositivo di stampa</b>	Include produttore, modello, descrizione, versione del firmware, numero di serie, identificativo della risorsa, nome del sistema, contatto, posizione, stato di gestione, workstation (desktop), numero di fax e nome coda.
<b>Indirizzo di rete del dispositivo di stampa</b>	Include indirizzo MAC, indirizzo IP, nome DSN, subnet mask, gateway IP predefinito, ultimo indirizzo IP conosciuto, indirizzo IP modificato, fuso orario, indirizzo IPX, numero di rete esterno IPX e server di stampa IPX.
<b>Proprietà del dispositivo di stampa</b>	Include componenti installati, descrizione dei componenti, funzionalità/servizi supportati, velocità di stampa, supporto stampa a colori, opzioni di finitura, supporto fronte/retro, tecnologia di marcatura, disco rigido, RAM, supporto per la lingua, proprietà definite dall'utente.
<b>Stato del dispositivo di stampa</b>	Include stato complessivo, avvisi dettagliati, messaggi della console locale, stato dei componenti, dati relativi allo stato di recupero dei dati, data di individuazione, tipo/metodo di individuazione, tempo di disponibilità del dispositivo, trap supportati/attivati.
<b>Contatori del dispositivo di stampa</b>	Include parametri di fatturazione, contatori di stampe, contatori di copie, contatori di fax, contatori di lavori di stampa di grandi dimensioni e contatori di scansioni, statistiche di utilizzo e volume di destinazione.
<b>Materiali di consumo del dispositivo di stampa</b>	Include il nome dei materiali di consumo, tipo (es: imaging, finitura, supporto carta), livello, capacità, stato, formato, ecc.
<b>Utilizzo dettagliato del dispositivo di stampa</b>	Dati di tracciabilità del lavoro di stampa relativi all'utente che includono caratteristiche del lavoro di stampa (ID, nome del documento, proprietario, tipo di documento, tipo di lavoro, colore, fronte/retro, supporti richiesti, formato, pagine, fascicoli, errori), destinazione (dispositivo di stampa, modello, nome DNS, indirizzo IP, indirizzo MAC, numero di serie), risultati della stampa del lavoro (ora di invio, ora di stampa, pagine stampate, pagine stampate a colori o in bianco e nero, modalità colori utilizzata, N-in-1), dati di contabilità (codice chargeback, prezzo di chargeback, fonte contabile), origine del lavoro di stampa (workstation, nome del server di stampa/indirizzo MAC, nome coda, porta, nome utente, ID utente), dati di gestione Xerox (inviati a Xerox® Services Manager).

Attributi dati	Descrizione dettagliata
<b>Identità di gestione del dispositivo</b>	Include informazioni sul PC host dell'applicazione, quali nome DNS, indirizzo IP, nome del sistema operativo, tipo di sistema operativo, tipo di processore, dimensioni della RAM (libera e utilizzata), dimensioni del disco rigido (spazio disponibile e spazio utilizzato), nome del sito, versione dell'applicazione, data di scadenza del contratto di licenza dell'applicazione, versione .Net, fuso orario, versione del componente di individuazione, dimensioni del database principale, dimensioni del database di individuazione, numero di stampanti incluse o meno nel contratto di assistenza di Xerox, servizi critici in esecuzione.
<b>Modo di protezione aziendale del Device Manager</b>	<p><b>Modalità normale</b> = Xerox® Device Agent contatta ogni giorno Xerox® Services Manager. È possibile cambiare in remoto le impostazioni senza l'esigenza di visite presso la sede del cliente quando le pianificazioni di polling sono disattivate.</p> <p><b>Modalità blocco</b> = a parte la sincronizzazione dei dati relativi alla stampante, non vi sono altre comunicazioni con Xerox® Services Manager e le impostazioni vanno modificate presso la sede del cliente. La macchina Xerox® Device Agent e gli indirizzi IP della stampante vengono riferiti a Xerox® Services Manager.</p>
<b>Criteri di controllo di stampa della gestione dei dispositivi</b>	Include nome del PC dell'utente finale, server di stampa utilizzato, coda di stampa utilizzata, data e ora della violazione, nome del documento, nome utente dell'utente finale, impostazione fronte/retro del lavoro di stampa, impostazione del colore del lavoro di stampa, impressioni totali del lavoro di stampa, prezzo del lavoro di stampa, azione intrapresa, utente finale notificato, messaggio visualizzato, nome della politica di stampa, regolamento della politica di stampa.

# Gestione in remoto dei dispositivi di stampa

Il personale di supporto Xerox® può elaborare le azioni seguenti attraverso l'applicazione di gestione dei dispositivi Xerox®. Se consentite, queste operazioni vengono eseguite a supporto delle attività di risoluzione delle anomalie, e sono delineate nella **Tabella 4** in basso.

Dati	Descrizione
Azioni da eseguire sui dispositivi di stampa	<ul style="list-style-type: none"> <li>• <b>Ottieni stato dispositivo</b> = recupera lo stato più recente del dispositivo di stampa</li> <li>• <b>Riavvia dispositivo</b> = avvia una sequenza di spegnimento/accensione sul dispositivo di stampa</li> <li>• <b>Aggiorna dispositivo</b> = installa nuovi software/firmware sul dispositivo di stampa (.DLM su porta 9100)</li> <li>• <b>Analisi problemi dispositivo</b> = esegue il ping del dispositivo e recupera l'ultimo stato dal dispositivo di stampa</li> <li>• <b>Stampa pagina di prova</b> = invia un lavoro di stampa di prova a un dispositivo di stampa per convalidare il percorso di stampa (genera un report di configurazione)</li> <li>• <b>Avvia gestione del dispositivo</b> = avvia trasferimenti periodici di dati del dispositivo di stampa ai server di comunicazione Xerox® esterni</li> </ul> <p><b>Nota:</b> nell'ambito della configurazione amministrativa delle applicazioni di gestione dei dispositivi Xerox® che supportano questa funzione, è possibile disabilitare ciascuna delle azioni dall'utilizzo su richiesta.</p>
Azioni da eseguire sui dispositivi di stampa	<ul style="list-style-type: none"> <li>• <b>Riavvia dispositivo</b> = avvia una sequenza di spegnimento/accensione sul dispositivo di stampa</li> <li>• <b>Stampa pagina di prova</b> = invia un lavoro di stampa di prova a un dispositivo di stampa per convalidare il percorso di stampa (genera un report di configurazione)</li> </ul>
Azioni da eseguire sulle applicazioni di gestione dei dispositivi	Le impostazioni all'interno di ciascuna applicazione di gestione dei dispositivi che possono essere gestite includono operazione di rilevamento, frequenza di esportazione dati, impostazioni relative alla comunicazione SNMP (riprova, timeout, nomi comunità), profili di avviso e frequenza di aggiornamento automatico del software di gestione dei dispositivi.



## Requisiti di sistema per le applicazioni di gestione dei dispositivi

I requisiti minimi variano leggermente a seconda delle offerte. Consultare la guida per l'utente, la guida per la valutazione della sicurezza e e/o la guida alla certificazione per i requisiti di base specifici della rispettiva applicazione di gestione dei dispositivi. Ulteriori dettagli sono disponibili all'indirizzo: <http://www.support.xerox.com/support/enus.html>

Al momento dell'installazione, viene incluso un file .readme che tratta i requisiti aggiuntivi e specifici di sistema per l'applicazione di gestione dei dispositivi che si sta installando.

- È consigliabile che sui computer host sia installato un sistema operativo supportato di Microsoft® Corporation. Tuttavia, le applicazioni di gestione dei dispositivi Xerox® possono essere eseguite in un ambiente Macintosh OS qualora si utilizzi il software di emulazione Parallels Desktop (attualmente non è possibile eseguire l'applicazione di gestione dei dispositivi in un ambiente Macintosh nativo). Per dettagli aggiuntivi, consultare le guide per l'utente della rispettiva applicazione di gestione dei dispositivi Xerox®.
- Si consiglia di mantenere aggiornati i computer host con le patch essenziali e le Service Release più recenti di Microsoft® Corporation.
- È necessario che il TCP/IP (Network Transmission Control Protocol/Internet Protocol) sia caricato e operativo.
- È richiesta una connessione a Internet.
- Sono richiesti privilegi di amministratore per installare il software dell'applicazione di gestione dei dispositivi sulla macchina client.
- Richiede dispositivi abilitati all'SNMP e la capacità di instradare l'SNMP sulla rete. Non è richiesto di attivare l'SNMP sul computer su cui verranno installate le applicazioni di gestione dei dispositivi Xerox® o su alcun computer nella rete.
- È necessario installare Microsoft®.NET Framework 4.6 (versione completa) prima di installare l'applicazione.
- L'applicazione non va installata su un PC su cui siano installate altre applicazioni basate su SNMP o altri strumenti di gestione dei dispositivi Xerox®, onde evitare reciproche interferenze nel funzionamento.

## Configurazioni non supportate

- Installazione dell'applicazione su computer con un'altra applicazione di gestione dei dispositivi Xerox®, quale Xerox® Device Manager.
- Qualsiasi sistema operativo Unix® o Linux®.
- Sistemi operativi Microsoft® alla fine del loro ciclo di vita, quali Windows NT® 4.0, Windows® Media Center, Windows® XP e Windows® Server 2000 e 2003.
- Ambienti virtuali diversi da VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Questa applicazione potrebbe funzionare in altri ambienti virtuali; tuttavia, tali ambienti non sono stati sottoposti a verifica.

## Processi aziendali Xerox® e servizi

I dati ricevuti dai server di comunicazione Xerox® provenienti da dispositivi di stampa Xerox® per ufficio, dispositivi di stampa Xerox® di produzione e applicazioni di gestione dei dispositivi Xerox® vengono utilizzati nei seguenti processi aziendali Xerox:

Nome del processo aziendale	Descrizione
<b>Letture dei consumi automatiche</b>	Una fattura viene generata automaticamente dai dati di consumo ricevuti dai dispositivi di stampa.
<b>Rifornimento automatico di materiali di consumo/ricambi</b>	Il toner viene inviato automaticamente ai clienti al ricevimento dello stato di esaurimento del materiale di consumo inviato dai dispositivi di stampa. I componenti sostituibili vengono inviati automaticamente ai clienti quando necessario.  Queste opzioni sono disponibili solo per i clienti che scelgono contratti di fornitura di materiali di consumo con rilevamento dati.
<b>Fruibilità (Assistente alla manutenzione)</b>	Le informazioni dettagliate sui guasti possono essere visualizzate dal personale di assistenza Xerox, laddove necessario, per velocizzare la preparazione di una visita presso la sede del cliente o diagnosticare e risolvere problemi a distanza.
<b>Supporto di 3° livello (Progettazione/Debug)</b>	Il personale di supporto del prodotto può eseguire il debug di problemi complessi quando ha accesso ai registri dettagliati di progettazione e debug.

I dati di base dei dispositivi di stampa vengono compressi, trasmessi, conservati e archiviati all'interno di un centro dati Xerox® certificato ISO-27001, e vengono conservati in conformità alle politiche di conservazione e gestione dei dati aziendali Xerox®.

I processi e le pratiche di lavoro che supportano e proteggono i sistemi software di back office Xerox® Remote Services sono basati sulle best practice ITIL e sulle politiche di protezione delle informazioni (IS) Xerox, che a loro volta si basano sugli standard ISO 27001. I clienti possono essere certi che la gestione dell'integrità, della privacy e della protezione dei dati è in linea con le best practice del settore.

# Dettagli tecnici

La presente sezione fornisce dettagli tecnici aggiuntivi che sono in genere richiesti dai team IT (Information Technology) e dai professionisti del settore della sicurezza al fine di gestire i rischi ottenendo la garanzia di pratiche di distribuzione protette; ciò consente la certificazione dei dispositivi di stampa e delle applicazioni di gestione dei dispositivi per l'utilizzo nell'ambiente di rete del cliente.

## Progettazione del software

L'impegno di Xerox® riguardo alla sicurezza dei propri prodotti inizia già nella fase di sviluppo, con best practice standard del settore in quanto a codifica protetta, verifiche esaustive e analisi per eliminare le vulnerabilità. Xerox® adotta attivamente criteri di certificazione quali Common Criteria, ed è attiva nel campo di standard emergenti quali P2600 Working Group e SDLC (Security Development Lifecycle).

## Operabilità

Xerox® Remote Services esegue i seguenti tipi di operazioni su una rete:

Metodo di distribuzione	Applicazioni utilizzate	Flusso di dati nella rete	Operabilità imposta su una rete
Device Direct	Nessuno	Interno	Il dispositivo di stampa Xerox® cerca di rilevare un server proxy Web (automatico o diretto 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 messaggi e-mail 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 suo certificato sul server di comunicazione Xerox remoto prima di trasmettere attributi dei 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® ogni giorno a un'ora specificata, oppure su richiesta del cliente.

Metodo di distribuzione	Applicazioni utilizzate	Flusso di dati nella rete	Operabilità imposta su una rete
		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 un elenco di azioni da eseguire (invia dati di fatturazione adesso, aggiungi servizio, ecc.).
		Esterno alla rete	Trasmissione unidirezionale su richiesta dei dati di registro progettazione del dispositivo di stampa Xerox® attraverso un canale crittografato (HTTPS sulla porta 443) al server di comunicazione Xerox®
Applicazioni di gestione dei dispositivi	Centre Ware® Web	Interno	Ogni applicazione individua un server proxy web (automatico o diretto a un indirizzo specifico)
		Interno	Ogni applicazione recupera le funzionalità dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Ogni applicazione recupera la configurazione dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Ogni applicazione recupera lo stato dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Ogni applicazione recupera i dati dei materiali di consumo dell'intero parco macchine tramite il protocollo SNMP
		Interno	Ogni applicazione può riavviare un dispositivo di stampa attraverso il protocollo SNMP o attraverso l'interfaccia utente Web del dispositivo di stampa
		Interno	Ogni applicazione può inviare una pagina di prova a uno specifico dispositivo di stampa
		Interno	Ogni applicazione può lanciare una pagina Web del dispositivo di stampa
		Esterno (solo in uscita)	Ogni applicazione attraversa il firewall dell'azienda 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 attributi dei dati
		Esterno (solo in uscita)	Ciascuna app 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 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

Metodo di distribuzione	Applicazioni utilizzate	Flusso di dati nella rete	Operabilità imposta su una rete
Applicazioni di gestione dei dispositivi	Xerox® Device Agent Partner Edition per il monitoraggio dei dispositivi di stampa collegati in rete	Interno	Ciascuna app Xerox® Device Agent rileva un server proxy Web (automatico o diretto a un indirizzo specifico)
		Interno	Ciascuna app Xerox® Device Agent recupera le funzionalità dei dispositivi dell'intero parco macchine attraverso il protocollo SNMP
		Interno	Ciascuna app Xerox® Device Agent recupera la configurazione dei dispositivi dell'intero parco macchine attraverso il protocollo SNMP
		Interno	Ciascuna app Xerox® Device Agent recupera lo stato dei dispositivi dell'intero parco macchine attraverso il protocollo SNMP
		Interno	Ciascuna app Xerox® Device Agent recupera i dati sui materiali di consumo dei dispositivi dell'intero parco macchine attraverso il protocollo SNMP
		Interno	Ciascuna app Xerox® Device Agent può richiedere che il dispositivo stampi un report di configurazione
		Interno	Ciascuna app Xerox® Device Agent può lanciare una pagina web del dispositivo di stampa
		Interno	Ciascuna app Xerox® Device Agent può aggiornare il software del dispositivo di stampa tramite l'invio di un lavoro di stampa. (file .DLM sulla porta 9100).
		Esterno (solo in uscita)	Ciascuna app 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 attributi dei dati
		Esterno (solo in uscita)	Ciascuna app Xerox® Device Agent trasmette automaticamente i dati degli attributi del dispositivo di stampa tramite 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 Xerox® tramite 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 diretto a un indirizzo specifico)
		Interno	Le app Xerox® Device Manager/Xerox® Device Agent recuperano le funzionalità dei dispositivi dell'intero parco macchine tramite il protocollo SNMP

Metodo di distribuzione	Applicazioni utilizzate	Flusso di dati nella rete	Operabilità imposta su una rete
Applicazioni di gestione dei dispositivi	Xerox® Device Manager per il monitoraggio dei dispositivi di stampa collegati in rete	Interno	Le app Xerox® Device Manager/Xerox® Device Agent recuperano la configurazione dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Le app Xerox® Device Manager/Xerox® Device Agent recuperano lo stato dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Le app Xerox® Device Manager/Xerox® Device Agent recuperano i materiali di consumo dei dispositivi dell'intero parco macchine tramite il protocollo SNMP
		Interno	Le app Xerox® Device Manager/Xerox® Device Agent possono richiedere che il dispositivo stampi un report di configurazione
		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 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® 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 attributi dei dati
		Esterno (solo in uscita)	Le app Xerox® Device Manager/Xerox® Device Agent trasmettono automaticamente i dati degli attributi 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 interrogano automaticamente i server di comunicazione Xerox® tramite un canale crittografato (HTTPS sulla porta 443) a un'ora specifica ogni giorno per un elenco di azioni da eseguire

## SNMP (Simple Network Management Protocol)

Il protocollo SNMP (Simple Network Management Protocol) è lo strumento di gestione di rete più diffuso per la comunicazione tra sistemi di gestione della rete e stampanti di rete. Le applicazioni di gestione dei dispositivi utilizzano il protocollo SNMP durante le operazioni di rilevamento per recuperare informazioni dettagliate sui dispositivi di stampa trovate sulla rete. Le applicazioni di gestione dei dispositivi Xerox® supportano i protocolli SNMP v1/v2 e v3. Consultare le guide alla certificazione delle rispettive applicazioni di gestione dei dispositivi Xerox® per i dettagli specifici.

L'infrastruttura SNMP v3 supporta più modelli di sicurezza, che possono coesistere simultaneamente all'interno di un'entità SNMP. Il protocollo SNMPv3 comprende una sicurezza più rigorosa, aggiungendo la sicurezza crittografica all'SNMPv2. Inoltre, il protocollo SNMPv3 è retrocompatibile con le versioni precedenti, e viene ampiamente utilizzato con reti robuste.

Le applicazioni di gestione dei dispositivi Xerox® (Centre Ware® Web/Xerox® Device Manager) sono in grado di comunicare con piattaforme per dispositivi che sono conformi allo standard FIPS 140-2 nelle loro implementazioni del protocollo SNMPv3.

Le applicazioni di gestione dei dispositivi Xerox® non utilizzano il servizio SNMP di Windows o il servizio trap SNMP di Windows. Tali servizi, se installati in precedenza **devono** essere disattivati su qualsiasi PC o server su cui sia installata l'applicazione di gestione dei dispositivi Xerox®.

Le applicazioni di gestione dei dispositivi Xerox® utilizzano un agente SNMP sviluppato da Xerox che:

- Contiene uno speciale meccanismo di codifica/decodifica
- È interamente gestito mediante .NET
- Utilizza l'eseguibile runtime .NET, che offre una maggiore sicurezza per impedire attacchi contro le vulnerabilità del software come manipolazioni di puntatori irregolari, sovraccarichi buffer e controllo dei limiti.

Le applicazioni di gestione dei dispositivi Xerox® utilizzano le funzioni di sicurezza disponibili nel sistema operativo Windows, tra cui:

- autenticazione e autorizzazione dell'utente
- configurazione e gestione dei servizi
- implementazione e gestione dei criteri di gruppo

ICF (Internet Connection Firewall) di Windows, che comprende:

- Impostazioni di registrazione della sicurezza
- Impostazioni ICMP

Applicazioni di gestione dei dispositivi Xerox®: **Xerox® Device Agent, Xerox® Device Agent Partner Edition o Xerox® Device Manager** utilizzano l'applicazione SQL CE Microsoft® SQL Server

È possibile configurare l'applicazione di gestione dei dispositivi Xerox® per sfruttare le funzionalità di protezione aggiuntive dell'applicazione Microsoft SQL® Server, tra cui:

- Abilitazione della registrazione dell'account utente
- Crittografia del DNS (Domain Name System)
- Limitazione dei privilegi account dell'utente per accedere al database (ad es: diritti di proprietà del database)
- Implementazione di numeri di porte definiti dall'utente

Sono richiesti un codice di registrazione Xerox e un account Xerox valido per trasmettere i dati ai server di comunicazione Xerox® remoti.

Le comunicazioni esterne delle applicazioni di gestione dei dispositivi Xerox® potrebbero subire effetti negativi dovuti al Firewall Connessione Internet di Windows (si **consiglia** ai clienti di inserire nella whitelist (indirizzi consentiti) l'URL di Xerox sul firewall del cliente e di specificare l'indirizzo IP che può accedere a tale URL.)

Le applicazioni di gestione dei dispositivi Xerox® vengono eseguite come un processo in background utilizzando le credenziali di account di un sistema locale per interrogare automaticamente i dispositivi di stampa della rete tramite il protocollo SNMP e ritrasmettere periodicamente gli attributi del dispositivo di stampa ai server di comunicazione Xerox®

L'accesso all'interfaccia utente (UI) e alle funzioni dell'applicazione Xerox® Device Manager (XDM) sono controllate tramite i seguenti privilegi basati sui ruoli (ad es. Centre Ware® Web Administrator, Centre Ware® Web Power User, Centre Ware® Web SQL User, Centre Ware® Web Customer Administrator e gruppi di Centre Ware® Web Customer forniti).

I nomi utente e le password per le applicazioni non attraversano la rete; sono invece utilizzati i token di accesso (come da progettazione del sistema operativo Windows®).

L'applicazione Xerox® Device Manager (XDM) offre una protezione basata sul controllo dell'invio in stampa limitando i lavori di stampa in base ai criteri di uso del colore, al tipo di documento, al costo del lavoro di stampa, all'ora del giorno, al controllo di accesso del gruppo di utenti, ai criteri fronte/retro, alle impressioni del lavoro di stampa consentite e alle quote di stampa.

**Note:** l'utilizzo di SNMP da parte di qualsiasi applicazione Xerox® Remote Services non dovrebbe comportare un rischio di sicurezza per l'ambiente IT di un cliente, poiché tutto il traffico basato su SNMP generato o consumato da queste applicazioni si verifica all'interno dell'intranet del cliente, dietro il firewall. Il servizio SNMP e il servizio trap SNMP di Windows non sono abilitati nel sistema operativo Windows per impostazione predefinita.

## Modalità di protezione aziendale

In aggiunta a qualsiasi sincronizzazione pianificata dalle applicazioni di gestione dei dispositivi Xerox® su Xerox® Services Manager, viene effettuata una sincronizzazione giornaliera come impostazione predefinita. Le due modalità di sicurezza aziendale esistenti sono la modalità **Normale** e la modalità **Blocco**.

In modalità **normale**, l'applicazione di gestione dei dispositivi contatta ogni giorno Xerox® Services Manager quando tutte le altre sincronizzazioni pianificate sono state disattivate (**modalità consigliata**).

In modalità **blocco**, oltre alla sincronizzazione dei dati relativi alle stampanti, non si verifica alcuna comunicazione con Xerox® Services Manager. Le modifiche a questa



impostazione devono essere effettuate presso la sede del cliente (**la sincronizzazione dei dati** assicura che le informazioni sui dispositivi di stampa inviate dall'applicazione di gestione dei dispositivi Xerox® e i dati che vengono acquisiti in Xerox® Services Manager coincidano).

Come impostazione predefinita, l'applicazione di gestione dei dispositivi Xerox® contatta ogni giorno Xerox® Services Manager e consente agli amministratori di modificare in remoto le impostazioni, evitando l'esigenza di chiamate di assistenza presso la sede del cliente. Si consiglia di non modificare questa impostazione. Qualora un cliente limiti il supporto in remoto dei dispositivi di stampa da parte del personale Xerox, è possibile bloccare la comunicazione dei dispositivi con Xerox® Services Manager, tranne che per la sincronizzazione dei dati delle stampanti. In questa modalità, l'applicazione non riferisce alcun indirizzo IP di computer o di stampante, né le impostazioni della sede a Xerox® Services Manager, e qualsiasi modifica alle impostazioni richiede una visita presso la sede del cliente.

**Nota:** se Xerox® Device Agent non contiene la scheda Modalità di protezione aziendale, funziona in modalità Normale.

## Protocolli, porte e altre tecnologie correlate

La seguente tabella identifica i protocolli, le porte e le tecnologie che vengono utilizzati all'interno di Xerox® Remote Services:

Numero di porta	Protocollo	Descrizione di utilizzo	Flusso dati sulla rete
Dipendente dai protocolli di livello superiore	Protocollo IP	Trasporto di base per tutte le comunicazioni dati	Interno + esterno (solo in uscita)
NA	Protocollo ICMP	Individuazione del dispositivo di stampa + risoluzione dei problemi	Interno
25	Protocollo SMTP	Dispositivo di stampa + avviso di notifica per e-mail dell'applicazione Remote Proxy	Interno
53	Protocollo DNS	Utilizzato per le operazioni di individuazione di dispositivi di stampa basate sul sistema DNS	Interno
80	HTTP (Hyper Text Transport Protocol)	Query delle pagine Web dei dispositivi di stampa + query delle pagine Web dell'applicazione di gestione dei dispositivi	Interno
135	Protocollo RPC	Individuazione del dispositivo di stampa	Interno
137, 139	Protocollo NetBIOS	Rilevamento dei server di stampa	Interno
161	Protocollo SNMP (SNMP v1 / v2C / v3)	Protocollo standard utilizzato per individuare i dispositivi di stampa collegati alla rete + Recupero di stato, contatori e dati sui materiali di consumo + Recupero e applicazione della configurazione del dispositivo di stampa. Nomi community predefiniti = "pubblico" (GET), "privato" (SET)	Interno

Numero di porta	Protocollo	Descrizione di utilizzo	Flusso dati sulla rete
162	Trap SNMP	Nome community predefinito = "SNMP_trap"	Interno
389	Protocollo LDAP	Individuazione del dispositivo di stampa attraverso l'enumerazione della partizione di Active Directory Microsoft Set di configurazione del servizio di digitalizzazione + Active Directory Customer Import + Configurazioni del customer group	Interno
443	HTTPS (Hyper Text Transport Protocol Secure)	Query delle pagine Web protette dei dispositivi di stampa (se configurate) + query delle pagine Web protette dell'app proxy remota (se configurata) +  Trasferimento dati del dispositivo di stampa ai server di comunicazione Xerox® + comunicazioni dei controlli di stampa a Xerox® Device Manager	Interno + esterno (solo in uscita)
452	Protocollo SAP	Individuazione del dispositivo di stampa utilizzando le query del server Novell attraverso il protocollo IPX	Interno
515, 9100, 2000, 2105	Invio del lavoro di stampa ai protocolli TCP/IP e LPW e alla porta RAW	Aggiornamento del software del dispositivo di stampa +  Diagnosi della pagina di prova	Interno
631	Protocollo IPP	Individuazione del dispositivo di stampa	Interno

## Procedure consigliate relative alla sicurezza

Aggiornare sempre i dispositivi di stampa con le versioni più aggiornate di firmware e software. Utilizzare l'interfaccia utente (UI) del dispositivo di stampa o l'applicazione di gestione del dispositivo di stampa fornita da Xerox® e da altri fornitori di stampa per aggiornare il firmware o il software del dispositivo di stampa.

Disabilitare le porte e i protocolli non utilizzati sui dispositivi di stampa ove possibile. Di solito questa procedura si applica all'interfaccia utente Web dei dispositivi di stampa da ufficio e all'interfaccia utente locale dei dispositivi di stampa di produzione.

Utilizzare le funzionalità di controllo dell'accesso utente sui dispositivi di stampa, se disponibili. Di solito questa procedura si applica all'interfaccia utente Web dei dispositivi di stampa da ufficio e all'interfaccia utente locale dei dispositivi di stampa di produzione.

Utilizzare protocolli protetti, quando possibile. Di solito questa procedura si applica all'interfaccia utente Web dei dispositivi di stampa da ufficio e all'interfaccia utente locale dei dispositivi di stampa di produzione.

Abilitare le funzionalità di protezione integrate nel dispositivo (sovrascrittura delle immagini, crittografia del disco, stampa protetta, ecc.)

Accertarsi che il firewall aziendale possa indirizzare i pacchetti HTTPS attraverso la porta 443, in conformità alle politiche di sicurezza dell'azienda.