Servicii la distanță @ Xerox

Cartea albă de securitate

Versiunea 4.0

martie 2022

IS 614672/IS 514590

Cuprins

1. Scop general și audiență

Cartea albă de securitate pentru servicii la distanță @Xerox este furnizată pentru a ajuta clienții să înțeleagă și să implementeze soluția securizată de servicii la distanță care funcționează cel mai bine cu construcția rețelei și politicile de securitate a informațiilor. Pentru a garanta cea mai sigură metodă de configurare, rețineți că pot fi necesare modificări la firewall-ul de Internet al clientului, la serverele proxy web sau alte infrastructuri de rețea ce țin de securitate

Publicul țintă pentru acest document include furnizori tehnici, manageri de rețea și specialiști în securitatea rețelei interesați de capabilitățile serviciilor de la distanță și de implementarea securității acestor caracteristici.

Vă recomandăm ca documentul să fie revizuit în întregime pentru a certifica utilizarea produselor și serviciilor Xerox® în mediul de rețea al unui client.

2. Propunere de valoare

Oferim o modalitate sigură și securizată pentru ca datele dispozitivului să fie trimise la sistemul nostru certificat ISO pentru a automatiza sarcinile comune și pentru a oferi o experiență mai bună a serviciilor de întreținere și asistență.

- Raportările contorului de facturare sunt automate și precise.
- Programul de reaprovizionare automată a consumabilelor oferă toner în funcție de nivelurile de toner raportate de imprimantă, astfel că nu este necesar să urmăriți inventarul ori să apelați pentru consumabile.
- Trimiterea informațiilor de diagnosticare ne ajută să oferim un suport mai bun pentru dispozitivul dvs., permițând adesea rezolvarea mai rapidă a problemelor.
- Anumite modele de imprimante pot verifica actualizările software importante și pot instala actualizările în mod programatic, fără intervenția clientului.Vezi nota
- Capacitățile noastre de gestionare a serviciilor oferă, de asemenea, o modalitate de a gestiona imprimantele non-Xerox, pe lângă imprimantele Xerox.
- Aceste servicii permit clienților noștri să-și utilizeze mai eficient timpul.

Toate acestea sunt realizate cu prioritizarea securității.

Notă: Această opțiune poate fi dezactivată pentru mediile în care clienții confirmă o versiune software setată și doresc să controleze software-ul de imprimare atunci când apar actualizări. Acest lucru se poate face fără ca dvs. să trebuiască să dezactivați capacitățile serviciilor la distanță rămase.

3. Servicii la distanță

Informația este un capital cheie iar securitatea este fundamentală pentru toate capitalurile organizației, inclusiv pentru dispozitivele de imprimare multifuncționale în rețea (MFP). În prezent, gestionarea unei flote de dispozitive de imprimare multifuncționale, asigurând în același timp un nivel acceptabil de securitate, prezintă un set de provocări unice, adesea trecute cu vederea. Noi înțelegem această complexitate și răspundem la nevoile de securitate ale clienților noștri. Produsele Xerox®, Sistemele Xerox® și ofertele de servicii la distanță sunt concepute pentru a se integra în siguranță cu fluxurile de lucru existente ale clienților noștri, utilizând în același timp cele mai recente tehnologii securizate.

În mod implicit, nu se transmit serverelor noastre imagini ale clienților din acțiuni de tipărire, fax, scanare, copiere sau alte informații sensibile.

Serverele Xerox din SUA se conformează cerințelor stricte de securitate pentru managementul securității informațiilor. Centrele noastre de date și aplicaţiile de servicii la distanță mențin Declarația anuală privind standardele de atestare (SSAE) nr. 16, cerințele de conformitate cu Sarbanes-Oxley Act (SOX) și sunt certificate ISO 27001:2013.

4. Modele de implementare

Clienții pot alege între următoarele modele de implementare Xerox® Remote Services, la fel de sigure:

- **Modelul combinat – (*Model preferat)*** Implementarea atât a modelului de aplicație Device Direct, cât și a modelului de gestionare a dispozitivelor împreună este ideal, deoarece oferă cele mai solide seturi de date și capabilități de gestionare a dispozitivelor.

- **Modelul Device Direct** - Device Direct permite dispozitivelor de imprimare să comunice direct cu serverele de comunicații Xerox® de la distanță prin Internet, prin firewall-ul clientului, pentru a oferi reaprovizionarea automată a consumabilelor (ASR), citirea automată a contorului (AMR) și rapoartele de diagnostic ale dispozitivului. Acest model de implementare oferă un set de elemente de date în sarcina utilă standard pentru a include defecțiuni ale dispozitivului, alerte, contoare, elemente de service de înaltă frecvență (HFSI) și alte atribute ale dispozitivului de imprimare.
- **Modelul aplicație de gestionare a dispozitivelor** - Aplicațiile Xerox® de gestionare a dispozitivelor pot fi implementate în rețeaua unui client pentru a colecta un set de atribute de date de la dispozitivele de imprimare pentru a oferi, de asemenea, reaprovizionarea automată a consumabilelor (ASR), citirile automate ale contorului (AMR) și rapoartele de diagnostic ale dispozitivului. Atributele dispozitivului de imprimare sunt colectate și apoi transmise în siguranță către serverele Xerox de la distanță. Atributele datelor de la dispozitivele de imprimare Xerox și non-Xerox pot fi comunicate ca parte a acestui model de implementare.

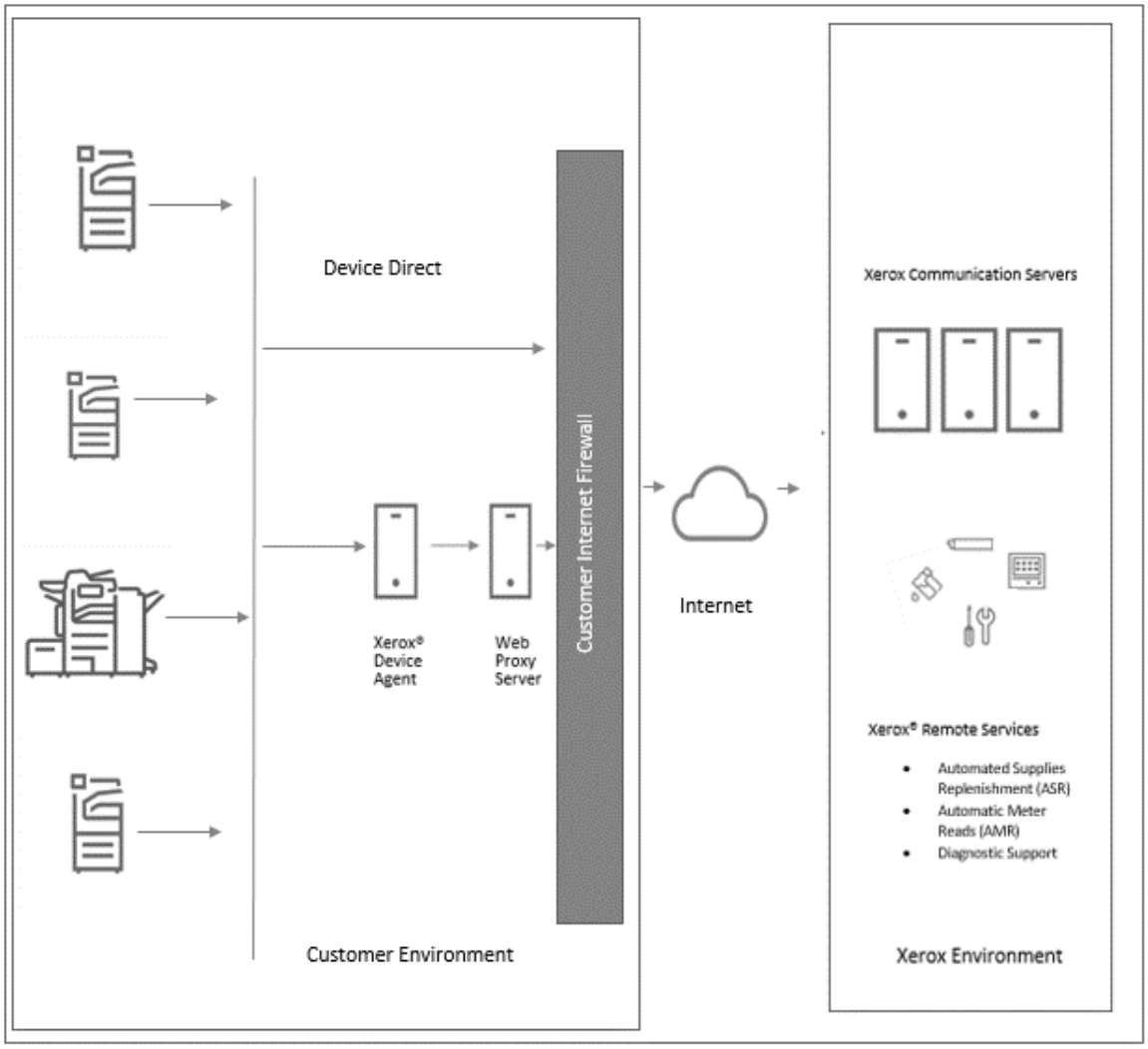
Toate modelele de implementare pentru Xerox® Remote Services sunt la fel de sigure și folosesc cele mai recente protocoale și porturi standard din industrie pentru a stabili un canal securizat și criptat atunci când se transmit atributele dispozitivului de imprimare extern către serverele Xerox la distanță situate în centrele noastre de date securizate redundante.

Modelul de implementare ales depinde de tipul de soluție de serviciu de imprimare al clienților noștri, de politicile de securitate a informațiilor și de regulile de manipulare a atributelor de transmitere a datelor dispozitivului de imprimare.

Modelul de implementare combinată (preferat)

Implementarea combinată se realizează atunci când un client achiziționează mai multe tipuri de contracte de întreținere Xerox pentru dispozitivele sale de imprimare și pentru a obține o soluție mai robustă de servicii la distanță. Atunci când un Xerox® Print Device este instalat inițial într-o rețea, comportamentul implicit al serviciilor de la distanță Xerox este ca dispozitivul de imprimare să încerce automat să comunice în exterior către serverele noastre de comunicații utilizând o metodă de conectare sigură și autentificată.

Figura 1



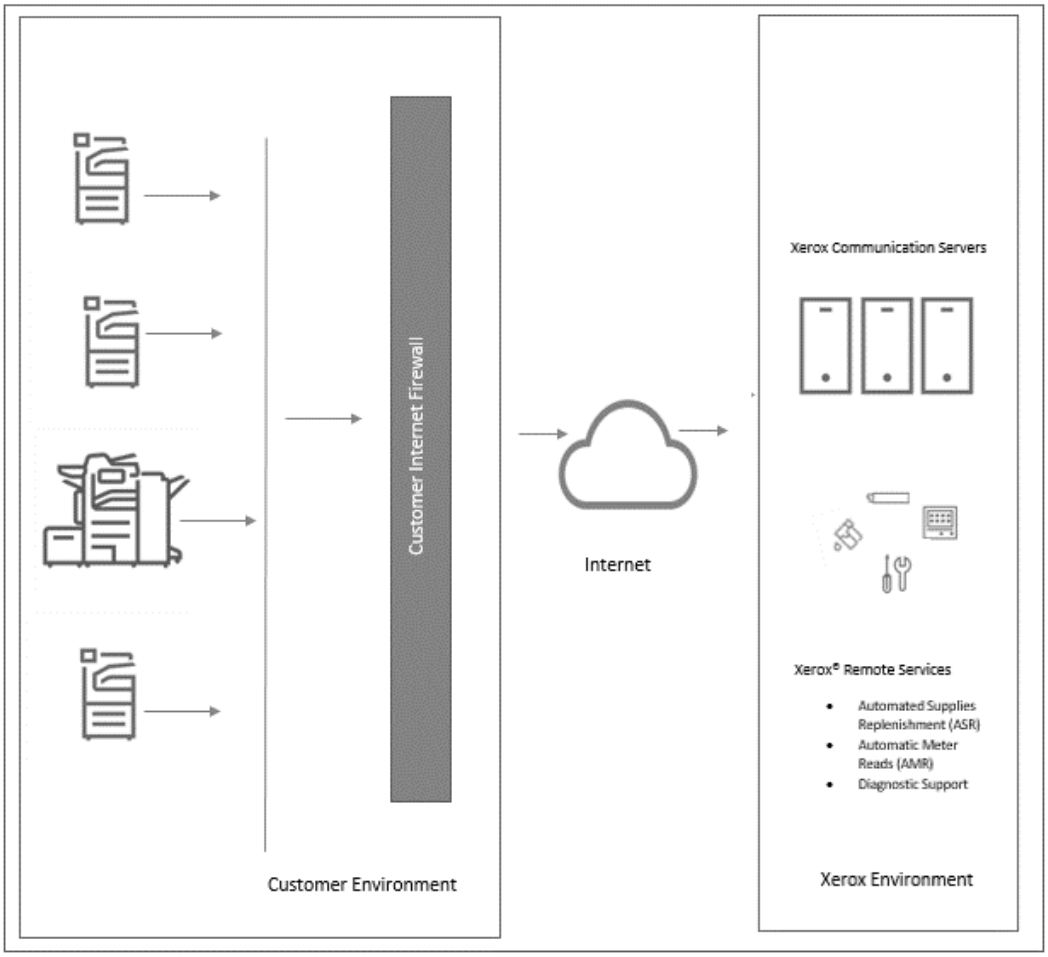
Combination Deployment Model

Model de implementare Device Direct

Dispozitivele Xerox® cu capabilități de Servicii la Distanță utilizează o conexiune de protocol Transport Layer Security (TLS) 1.2 prin portul standard securizat 443 pentru a comunica la ieșire către serverele noastre securizate.

- Dispozitivele de imprimare din mediul clientului inițiază toate comunicațiile cu serverele de comunicații. Configurațiile standard ale firewall-ului de pe site sunt necesare pentru a permite comunicarea.
- Trebuie utilizat un URL valid pentru serverele de comunicații (*.xerox.support.com) pentru a autentifica dispozitivele de imprimare în infrastructura Xerox
- Dispozitivul solicită înregistrarea pe serverele de comunicații utilizând acreditările corespunzătoare pentru autentificarea certificatelor.
- Serverele de comunicare validează acreditările furnizate de imprimante și acceptă solicitările.
- Serverele de comunicații se află în spatele unui firewall securizat și nu sunt accesibile de pe Internet.

Figura 2



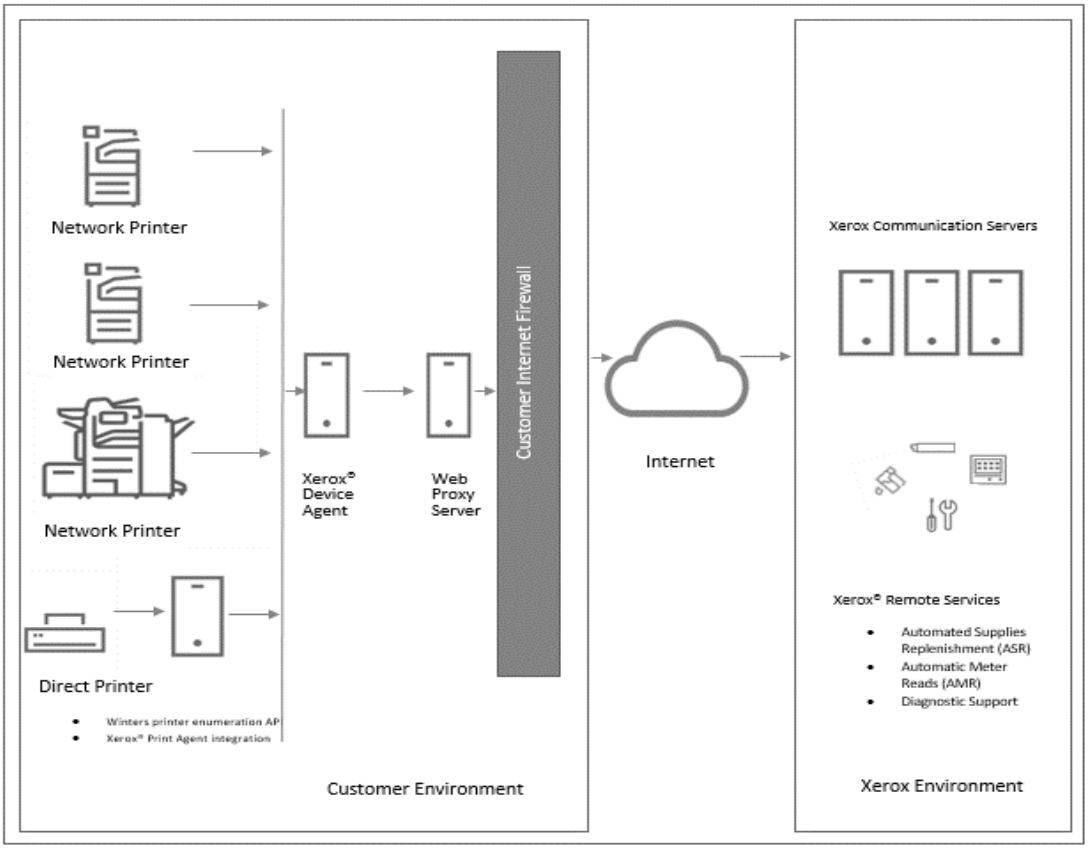
Device Direct Deployment Model

Model de implementare a aplicațiilor de gestionare a dispozitivelor

Aplicațiile de gestionare a dispozitivelor (adică **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **și Xerox Device Manager**) utilizează o conexiune Transport Layer Security (TLS) 1.2 Protocol prin portul standard securizat 443, pentru a comunica extern cu serverele de comunicații. Funcțiile suplimentare sunt utilizate pentru a îmbunătăți securitatea pe acest canal și sunt stabilite în timpul instalării inițiale a aplicațiilor de gestionare a dispozitivelor, care includ:

- Aplicația de gestionare a dispozitivului din mediul clientului inițiază toate comunicațiile cu serverele de comunicații. Configurațiile standard ale firewall-ului de pe site sunt necesare pentru a permite comunicarea.
- Serverele de comunicare validează acreditările furnizate de imprimante și acceptă solicitările.
- Aplicația de gestionare a dispozitivului solicită înregistrarea pe serverele de comunicații utilizând acreditările corespunzătoare pentru autentificarea certificatelor.
- Serverele de comunicare validează acreditările furnizate de imprimante și acceptă solicitările.
- Aplicația de gestionare a dispozitivului autentifică serverele de comunicații și activează serviciul.

Figura 3



Device Management Application Deployment Model

5. Transmiterea datelor și sarcinile utile de plată

Surse de date

Atributele de date ale dispozitivului de imprimare care sunt trimise ca parte a sarcinii utile de plată transmise provin din următoarele surse:

- Imprimante de rețea Xerox® Office
- Imprimante de rețea non Xerox
- Imprimante Xerox® Production
- Aplicații Xerox® Device Management

Notă: Nu toate imprimantele de producție Xerox Office și Xerox sunt capabile de servicii Xerox la distanță. Puteți găsi o listă completă de produse performante aici. Atributele dispozitivului de imprimare variază în funcție de produs și de soluția de implementare Xerox® Remote Services.

Dispozitive de birou Xerox®

Tabelul 1 Identifică atributele de date ale dispozitivului care pot fi transmise pentru produsele Xerox® Office compatibile cu servicii la distanță.

Atribute de date	Descrierea detaliată a atributelor datelor
dentitatea dispozitivului de imprimare	Include modelul, nivelurile de firmware ale modulelor, numerele de serie ale modulelor, datele de instalare ale modulelor, datele de licențiere și locația, dacă sunt disponibile.
Adresa de rețea a dispozitivului de imprimare	Include adresa MAC (Media Access Control), adresa de subrețea.
Proprietățile dispozitivului de imprimare	Include configurația detaliată a componentelor hardware, configurația detaliată a modulelor software, caracteristicile/serviciile acceptate etc.
Starea dispozitivului de imprimare	Include stări active, istoricul defecțiunilor, jurnalul de evenimente DFE, istoricul transmisiilor de date
Contoarele dispozitivului de imprimare	Include contoare de facturare, contoare legate de imprimare, contoare legate de copiere, contoare mari legate de lucrări, contoare specifice producției, contoare legate de scanare către destinație pe modele de producție de gamă inferioară etc.
Consumabilele dispozitivului de imprimare	Include producătorul, modelul, numărul de serie, nume, tip, nivel, capacitate, stare, contoare pentru întreaga durată de funcționare etc.
Utilizarea detaliată a mașinii de imprimare	Include date HFSI, date NVM, înlocuirea pieselor, jurnale DFE, date detaliate de diagnosticare, rezolvarea defecțiunilor.
Inginerie / Depanare	Include date nestructurate, detaliate, legate de depanare, destinate numai pentru nivelul 3 de asistență.

Atribute de date	Descrierea detaliată a atributelor datelor
Privitor la lucrările clientului	Produsele de imprimare Xerox® Production oferă capacitatea de a reproduce datele legate de lucrări în sprijinul scenariilor de asistență transmise mai departe prin PostScript criptat către Xerox. Clientul poate controla dacă să activeze sau nu această caracteristică. Dacă clientul alege să transmită înapoi către Xerox date legate de lucrări (adică PostScript criptat), acele date sunt gestionate în conformitate cu politicile și standardele Xerox privind securitatea informațiilor (IS).

Dispozitivele noastre de imprimare de tip office transmit atributele datelor dispozitivului într-un format XML (eXtensible Markup Language) folosind un fișier .zip comprimat. Odată autentificat, fiecare fișier este apoi transmis printr-un canal criptat către serverele de comunicații.

Dispozitive Xerox® Production

Tabelul 2 Identifică atributele de date ale dispozitivului care pot fi transmise pentru produsele Xerox® Production capabile de servicii la distanță.

	Descriere
Identitatea dispozitivului de imprimare	Include modelul, nivelul firmware-ului, numerele de serie ale modulelor și data instalării.
Adresa de rețea a dispozitivului de imprimare	Include adresa de control al accesului media (MAC), adresa de subrețea.
Proprietățile dispozitivului de imprimare	Include configurația detaliată a componentelor hardware, configurația detaliată a modulelor software, caracteristicile/serviciile acceptate, moduri de economisire a energiei etc.
Starea dispozitivului de imprimare	Include starea generală, alerte detaliate, istoricul ultimelor 40 de defecțiuni, date despre blocaje etc
Contoarele dispozitivului de imprimare	Include contoare de facturare, contoare legate de imprimare, contoare legate de copiere, contoare legate de fax, contoare mari legate de lucrări, contoare legate de scanare la destinație, statistici de utilizare etc
Consumabilele dispozitivului de imprimare	Include denumirea consumabilului, tipul (de exemplu, imagistică, finisare, suport de hârtie), nivelul, capacitatea, starea, mărimea etc.
Utilizarea detaliată a mașinii de imprimare	Include contoare detaliate legate de imprimare, stări de pornire, cantități de înlocuire unități detaliate înlocuibile pentru clienți (CRU), informații detaliate de eroare CRU și distribuții, utilizarea caracteristicilor opțiunii de recunoaștere optică încorporată a caracterelor (OCR), distribuția lungimii de rulare a imprimării, distribuția utilizării tăvii de hârtie, media instalată, distribuția tipurilor de media, distribuția dimensiunii suportului media, distribuția lungimii documentului, numărul setat, datele HFSI, datele NVM, distribuția, numărul marcat de pixeli, acoperirea medie a suprafeței per culoare, defecțiuni/blocaje, contoare detaliate legate de scanare.
Inginerie / Depanare	Include informații detaliate de depanare care pot include date în afara setului de date enumerat mai sus. Aceste date pot include PII, cum ar fi nume de utilizator, adrese de e-mail și date despre lucrări. Aceste date sunt trimise numai cu permisiunea exprimată a clientului și sunt destinate utilizării numai pentru asistență la depanare secundară.

Dispozitivele noastre de imprimare din clasa de producție transmit atributele datelor dispozitivului într-un format XML (eXtensible Markup Language) folosind un fișier .zip comprimat. Odată autentificat, fiecare fișier este apoi transmis printr-un canal criptat către serverele pentru servicii la distanță.

Notă: Fișierul și conținutul datelor identificate variază în funcție de modelul produsului.

Aplicații de gestionare a dispozitivelor Xerox®

Sunt disponibile mai multe opțiuni de aplicații de gestionare a dispozitivelor, în funcție de mediul de rețea al clienților și de nevoia de gestionare a dispozitivelor de imprimare. Fiecare dintre acestea este la fel de sigură și are capacități robuste de gestionare a dispozitivelor de imprimare.

Mai jos găsiți o listă de aplicații de gestionare a dispozitivelor: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition și Xerox Device Manager.

Fiecare aplicație se sincronizează, implicit, cel puțin zilnic cu serverele de comunicații securizate. Pentru a asigura securitatea maximă pentru datele dumneavoastră, serverele de comunicații sunt găzduite într-o facilitate conformă cu ISO 27001. Datele trimise sunt, în primul rând, contoare de facturare specifice imprimantei, niveluri de aprovizionare și alerte de imprimantă. Datele sunt comprimate, criptate și protejate prin mai multe mecanisme:

- Aplicația de gestionare a dispozitivelor Xerox inițiază toate contactele cu serverele de comunicații Xerox iar pentru a permite comunicarea sunt necesare configurații standard de firewall în mediul clientului.
- Aplicațiile de gestionare a dispozitivelor Xerox necesită un proxy valid, în cazul în care este necesar un proxy pentru comunicarea prin Internet.
- Serverele de comunicații Xerox sunt protejate de un firewall securizat în mediul Xerox și nu sunt accesibile de pe Internet.
- Accesul la interfața cu utilizatorul a serverului de comunicații Xerox necesită autentificare. Informațiile despre gazda aplicației de gestionare a dispozitivelor Xerox sunt stocate într-un cont specific site-ului clientului, iar accesul la datele contului respectiv pe serverele de comunicații Xerox este limitat administratorilor de cont ai serverelor de comunicații Xerox.
- Toate comunicațiile serverului de comunicații Xerox sunt înregistrate și disponibile pentru vizualizare.
- Datele trimise către dispozitivele dvs. de imprimare din rețea, atunci când sunt activate, constau în principal din comenzi de la distanță care permit unui administrator de asistență de cont să solicite execuția la nivel de comandă a aplicației de gestionare a dispozitivelor Xerox în timpul scenariilor de asistență secundare.
- Solicitările implică în principal actualizări de firmware, repornirea imprimantei, imprimarea paginilor de testare și reîmprospătarea stării curente a dispozitivului.
- Aplicația de gestionare a dispozitivelor Xerox interogează periodic contul de servere de comunicații Xerox cu privire la solicitările de comandă.
- Rezultatele operațiunilor din solicitările de comandă sunt trimise la serverele de comunicații Xerox, unde sunt apoi revizuite.

Notă: Există o singură cerință de înregistrare la instalarea software-ului. Aceste informații de înregistrare includ un câmp pentru locația dispozitivului și adresa de e-mail de contact.

Aplicațiile de gestionare a dispozitivelor Xerox **(de exemplu, Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition și Xerox Device Manager)** transmit datele despre atributele de imprimare în format XML (eXtensible Markup Language) folosind un fișier .zip comprimat. Fișierul este apoi criptat și transmis prin canale criptate către serverele de comunicații de la distanță.

Tabelul 3 identifică o listă a atributelor de date ale dispozitivului și o descriere care pot fi trimise prin intermediul aplicației Xerox® Device Mgmt.

Atribute date	Descrierea detaliată a atributelor datelor
Identitatea dispozitivului de imprimare	Include producătorul, modelul, descrierea, nivelul firmware-ului, numărul de serie, etichetele funcțiilor, numele sistemului, contactul, locația, starea de gestionare a stației de lucru (desktop), numărul de telefon de fax și denumirea șirului.
Adresa de rețea a dispozitivului de imprimare	Include adresa MAC, adresa IP, numele DNS, masca de subrețea, gateway IP implicit, ultima adresă IP cunoscută, adresa IP schimbată, fusul orar, adresa IPX, numărul de rețea externă IPX, serverul de imprimare IPX.
Proprietățile dispozitivului de imprimare	Include componente instalate, descrieri ale componentelor, caracteristici/servicii acceptate, viteza de imprimare, suport pentru culori, opțiuni de finisare, suport duplex, tehnologie de marcare, hard disk, RAM, suport pentru limbă, proprietăți definite de utilizator.
Starea dispozitivului de imprimare	Include starea generală, alertele detaliate, mesajele consolei locale, starea componentelor, datele referitoare la regăsirea stării, data descoperirii, metoda/tipul descoperirii, ora de activare a dispozitivului, capcane acceptate/activate.
Contoarele dispozitivului de imprimare	Include contoare de facturare, contoare legate de imprimare, contoare legate de copiere, contoare legate de fax, contoare mari legate de lucrări, contoare legate de scanare, statistici de utilizare și volum țintă.
Consumabilele dispozitivului de imprimare	Include denumirea produsului consumabil, tipul (de exemplu, imagistică, finisare, suport de hârtie), nivelul,capacitatea, statutul, dimensiunea și atributele conexe
Utilizare detaliată a dispozitivului de imprimare	Date de urmărire a sarcinii de lucru referitoare la utilizator, care includ caracteristicile lucrării (ID-ul, numele documentului, proprietarul, tipul documentului, tipul operației, culoare, duplex, media necesare, dimensiune, pagini, seturi, erori), destinație (dispozitiv de imprimare, model, nume DNS, adresa IP, adresa MAC, numărul de serie), rezultatele tipăririi lucrării (timpul de solicitare, timpul de imprimare a lucrării, paginile tipărite, paginile color/alb-negru imprimate, modul de culoare utilizat, N-up), date contabile (cod de rambursare, preț de rambursare, sursă calcul), sursa lucrării de imprimare (stație de lucru, nume server de imprimare/adresă MAC, numeșsir, port, nume de utilizator, ID utilizator), informații de management Xerox (trimise către Xerox Services Manager).
Identitatea de gestionare a dispozitivului	Include informații despre PC-ul gazdă al aplicației, cum ar fi numele DNS, adresa IP, numele sistemului de operare, tipul sistemului de operare, procesorul PC-ului, dimensiunile RAM (liber vs. folosit), dimensiunile unității hard disk (liber vs. folosit), numele site-ului, versiunea aplicației, data de expirare a licenței aplicației, versiunea .Net, fusul orar, versiunea componentei de descoperire, dimensiunea bazei de date principale, dimensiunea bazei de date de descoperire, numărul de imprimante/în sfera de aplicare/în afara sferei de aplicare, servicii critice care rulează.
Manager dispozitive Modul de securitate al corporației	Modul normal = Xerox Device Agent contactează Xerox Services Manager, zilnic. Setările pot fi modificate de la distanță fără a fi nevoie de vizite la fața locului, chiar și atunci când programele de interogare sunt oprite. Mod de blocare = în afară de sincronizarea datelor legate de imprimantă, nu există comunicare cu Xerox Services Manager, iar setările trebuie modificate la fața locului. Adresele IP ale aparatului Xerox Device Agent și ale imprimantei sunt raportate la Xerox Services Manager.

Atribute date	Descrierea detaliată a atributelor datelor
Managementul dispozitivului Politici de control al imprimării	Include numele PC-ului utilizatorului final, serverul de imprimare utilizat, coada de imprimare utilizată, marca temporală a încălcării, numele documentului, numele de utilizator final, duplex operație, culoarea operației, afișări totale ale lucrării, prețul operației, acțiunile întreprinse, utilizatorul final notificat, mesajul afișat, denumirea politicii de imprimare, regula politicii de imprimare.

6. Gestionarea la distanță a dispozitivelor de imprimare

Personalul de suport secundar Xerox poate procesa următoarele acțiuni prin intermediul aplicațiilor Device Direct sau de gestionare a dispozitivelor Xerox.

Tabelul 4 prezintă eforturile sporite de soluționare, permise de client într-o situație de asistență secundară. Permisiunea clientului pentru a îndeplini aceste funcții trebuie să fie obținută în mod explicit.

Date	Descriere
Acțiuni de efectuat pe dispozitive de imprimare	• Aflare stare dispozitiv = recuperați cea mai recentă stare de pe dispozitivul de imprimare • Repornire dispozitiv = inițiați o secvență de oprire/repornire a alimentării dispozitivului de imprimare • Actualizare dispozitiv = instalați software/firmware nou pe dispozitivul de imprimare (.DLM prin portul 9100) • Depanare dispozitiv = dispozitiv ping + preluare cea mai recentă stare de la dispozitivul de imprimare • Imprimare pagină test = trimiteți o operație de testare la un dispozitiv de imprimare pentru a valida calea de imprimare (generați un raport de configurare) • Începere gestionare dispozitiv = inițiați transferuri periodice de date ale dispozitivului de imprimare către serverele Xerox® Communication externe **Notă: Fiecare acțiune poate fi dezactivată de la utilizare la cerere în cadrul porțiunii de configurare a administrării aplicațiilor de gestionare a dispozitivelor Xerox® care acceptă această caracteristică.**
Acțiuni de efectuat în aplicațiile de management al dispozitivelor	Setările din cadrul fiecărei aplicații de management al dispozitivelor care pot fi gestionate includ operațiunea de descoperire, frecvența de export de date, setările legate de comunicarea SNMP (reîncercare, expirare, numele comunităților), profiluri de alertă și frecvența de gestionare automată a dispozitivelor prin reactualizări software automate.

Date	Descriere
Gestionarea software la distanță	Anumite dispozitive sunt echipate cu capabilități automate de gestionare a software-ului la distanță. Aceste dispozitive trimit o interogare mediului Xerox pentru a vedea dacă există noi actualizări de software disponibile pentru dispozitiv. Dacă există, dispozitivul va putea trimite apoi o solicitare pentru acea actualizare a software-ului și va fi actualizat la ora stabilită. Cu toate acestea, dacă mediul dvs. interzice actualizările automate de software, opțiunea de gestionare a software-ului la distanță poate fi deselectată numai fără întreruperea serviciilor standard de la distanță.

Cerințe de sistem pentru aplicațiile de gestionare a dispozitivelor

Cerințele minime variază ușor în funcție de oferte. Consultați Ghidul utilizatorului, Ghidul de evaluare a securității și/sau Ghidul de certificare pentru cerințele de bază specifice aplicațiilor de gestionare a dispozitivelor respective.

La instalare, este inclus un fișier readme pentru a răspunde cerințelor de sistem suplimentare și specifice pentru aplicația de gestionare a dispozitivului care este instalată.

- Aplicațiile de gestionare a dispozitivelor sunt compatibile cu caracteristicile de securitate încorporate în sistemul de operare Windows®. Acestea se bazează pe un serviciu Windows® de fundal, care rulează sub acreditările contului de sistem local, pentru a permite monitorizarea proactivă a imprimantelor și a atributului de date de imprimare care va fi transmis către Xerox. Interfața cu utilizatorul care afișează sarcina utilă de plată a atributului datelor de imprimare este accesibilă numai utilizatorilor împuterniciţi și administratorilor cu acces la sistemul de operare Windows®.

- Pentru a preveni o întrerupere a comunicațiilor automate ale serviciilor de la distanță, se recomandă ca aplicația de gestionare a dispozitivelor să fie încărcată pe un client care este alimentat continuu sau în timpul orelor de lucru principale.

- Vă recomandăm ca computerele gazdă să ruleze un sistem de operare acceptat de la Microsoft® Corporation. Cu toate acestea, aplicațiile de gestionare a dispozitivelor Xerox pot fi rulate pe Apple® OS 10.9.4 sau o versiune ulterioară utilizând software-ul de emulare Parallels Desktop. Aplicația nu va rula în mediul nativ Macintosh. Consultați ghidurile utilizatorului corespunzătoare pentru asistență detaliată. Pot fi găsite cerințele pentru a rula pe un sistem de operare Macintosh.

- Vă recomandăm ca computerele gazdă să fie la zi cu cele mai recente corecții critice și versiuni de servicii de la Microsoft® Corporation.

- Protocolul de control al transmisiei în rețea/Protocolul Internet (TCP/IP) trebuie să fie încărcat și operațional.

- Sunt necesare privilegii administrative pentru a instala software-ul aplicației de gestionare a dispozitivelor pe computerul client.

- Necesită dispozitive cu SNMP activat și capacitatea de a ruta SNMP prin rețea. Nu este necesar să activați SNMP pe computerul pe care vor fi instalate aplicațiile de gestionare a dispozitivelor Xerox® sau pe orice alte computere din rețea.

- Microsoft®.NET Framework trebuie instalat înainte de a instala aplicația.

- Aplicația nu trebuie instalată pe un computer pe care sunt instalate alte aplicații bazate pe SNMP sau alte instrumente de gestionare a imprimării Xerox®, deoarece acestea pot interfera cu funcționarea celeilalte.

Configurații baze de date

- Aplicația instalează motorul de bază de date SQL Server Compact Edition (SQL CE) și fișierele de bază de date care stochează datele imprimantei și setările aplicației în directorul de instalare. Nu este necesară licențierea bazei de date pentru aplicație. Xerox® Device Agent acceptă, de asemenea, instanțe existente ale SQL Server, așa cum este descris mai sus.

Configurații neacceptate

Această secțiune descrie configurațiile care nu sunt acceptate.

- Instalarea aplicației pe un computer cu o altă aplicație de gestionare a dispozitivelor Xerox, cum ar fi Xerox Device Manager.

- Software-ul sistemului de operare nativ Mac OS® (de exemplu, Xerox Device Agent poate rula numai pe platforma Apple Mac atunci când este instalat software-ul Parallels Emulation.)

- Orice versiune de sisteme de operare UNIX®, sisteme de operare Linux®, sisteme Windows® care rulează clientul Novell, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Window® 2000, Windows® Server 2008 și 2008 R2, Windows® Server 2003, Windows® 8 RT, sisteme de operare care rulează Terminal Services pentru aplicații și sisteme Installation on Windows care rulează controlere de domeniu.

Deoarece această aplicație a fost testată numai pe mediul VMware® Lab Manager/stație de lucru, nu sunt acceptate alte medii virtuale.

7. Procese și servicii comerciale Xerox®

Datele primite de la dispozitivele de imprimare Xerox® Office, dispozitivele de imprimare Xerox® Production și aplicațiile de gestionare a dispozitivelor Xerox ca parte a soluției de servicii la distanță sunt utilizate de procesele de afaceri Xerox enumerate mai jos:

Tabelul 5 detaliază numele și descrierea procesului de afaceri și a serviciilor care sunt acceptate ca parte a soluției Servicii la distanță.

Numele procesului de afaceri	Descriere
Citiri automate ale contorului	Datele citite de contor sunt utilizate în procesul de facturare.
Aprovizionarea automată a consumabilelor / Aprovizionarea automată a pieselor	Tonerul este trimis automat clienților în funcție de starea de epuizare a consumabilelor, primită de la dispozitivele de imprimare. Anumite componente înlocuibile sunt livrate automat clienților atunci când sunt necesare pentru dispozitivele lor de imprimare. Aceste opțiuni sunt disponibile doar clienților care optează pentru contracte de furnizare cu contorizare.
Mentenanță (asistent de întreținere)	Gestionarea de la distanță a dispozitivului oferă informații detaliate despre defecțiuni care pot fi vizualizate de personalul de mentenanță Xerox, atunci când este necesar, pentru a accelera pregătirea pentru o vizită la fața locului sau pentru a diagnostica și rezolva problemele.
Suport nivel 3 (inginerie/depanare)	Personalul de asistență pentru produse poate depana probleme dificile atunci când are acces la jurnalele de inginerie detaliate și de depanare.
Dezvoltare produs	Datele privind performanța și utilizarea imprimantei sunt utilizate pentru a identifica îmbunătățirile produsului pentru versiunile viitoare.

Datele de bază ale dispozitivului de imprimare sunt agregate, transmise, păstrate și arhivate într-un centru de date Xerox certificat ISO-27001 și sunt păstrate în conformitate cu politicile de gestionare a reținerii datelor corporative Xerox.

Procesele și practicile de lucru care suportă și protejează sistemele software pentru servicii de la distanță se bazează pe cele mai bune practici ITIL și pe Politicile Xerox de securitate a informaţiilor, care se aliniază direct cu standardele ISO 27002 ale Organizației Internaționale de Standardizare a sistemului de management al securității informațiilor. Clienții pot fi asigurați că gestionarea, protecția și stocarea datelor dispozitivului se fac cu înțelegerea principiilor de bază ale securității informațiilor: confidențialitate, integritate, disponibilitate, autentificare și non-repudiere.

8. Detalii de tehnologie

Această secțiune oferă detalii tehnice suplimentare, solicitate de obicei de către echipele de tehnologie a informației (IT) și de practicienii în securitate care gestionează riscurile, garantând astfel practici de dezvoltare sigure. O astfel de asigurare le permite să certifice dispozitivele noastre de imprimare și aplicațiile de gestionare a dispozitivelor, pentru a fi utilizate în mediul de rețea al clientului.

Proiectare software

Angajamentul nostru vizavi de securitatea produselor Xerox începe devreme în dezvoltarea produsului, iar dezvoltatorii Xerox urmează un ciclu de viață formal de dezvoltare a securității care gestionează problemele de securitate prin identificare, analiză, prioritizare, codare și testare. Multe dispozitive de imprimare Xerox® sunt certificate conform criteriilor comune ISO IEC 15408 ori sunt în mod activ în curs de revizuire a certificării.

Operabilitate

Serviciile la distanță Xerox efectuează următoarele tipuri de operațiuni într-o rețea. Aceste operațiuni depind de metoda de implementare configurată.

Tabelul 6.

Metodă de implementare	Aplicație utilizată	Flux de date în rețea	Operabilitate impusă unei rețele
Dispozitiv Direct	Niciunul	Intern	Dispozitivul Xerox® de imprimare încearcă să detecteze un server proxy web (automat sau direcționat către o anumită adresă)
		Intern	Dispozitivele Xerox® de imprimare pot fi programate pentru a genera cereri către un server SMTP (Simple Mail Transport Protocol) pentru a trimite mesaje e-mail cu notificări de avertizare către o listă definită de destinatari
		Extern rețelei	Dispozitivul de imprimare Xerox® traversează firewall-ul companiei pentru a accesa Internetul (HTTPS prin portul 443)
		Extern rețelei	Dispozitivul Xerox® de imprimare se autentifică cu certificatul său la Xerox Communication Server la distanță înainte de a transmite orice atribut de date
		Extern rețelei	Dispozitivul Xerox® de imprimare transmite automat datele despre atributele dispozitivului de imprimare printr-un canal criptat (HTTPS prin portul 443) către Xerox® Communication Servers la o oră specificată zilnic sau la cererea clientului.
		Extern rețelei	Dispozitivul Xerox® de imprimare interogează automat Xerox® Communication Servers printr-un canal criptat (HTTPS prin portul 443) la o anumită oră în fiecare zi cu privire la o listă de acțiuni de efectuat (de exemplu, trimiterea datelor de facturare acum, adăugare serviciu etc.)

Metodă de implementare	Aplicaţie utilizată	Flux de date în rețea	Operabilitate impusă unei rețele
		Extern rețelei	Transmiterea la cerere unidirecţională a datelor din jurnalul de inginerie al dispozitivului Xerox® de imprimare printr-un canal criptat (HTTPS prin portul 443) către Xerox® Communication Server
Dispozitiv Direct	Niciunul	Ieșire, inițiat de dezvoltator pentru a extrage cele mai recente programe software	Dispozitivul trimite interogare către serverul de gestionare a software-ului de la distanță pentru a verifica dacă există actualizări de software/securitate. Dacă mediul clientului interzice actualizările automate de software, opțiunea de gestionare a software-ului la distanță poate fi deselectată numai fără întreruperea serviciilor standard de la distanță.
Aplicații de gestionare a dispozitivelor	Centrul Ware® Web	Intern	Fiecare aplicație detectează un server proxy web (automat sau direcționat către o anumită adresă)
		Intern	Fiecare aplicație preia capabilitățile dispozitivului de imprimare din întreaga flotă prin SNMP
		Intern	Fiecare aplicație preia configurația dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Fiecare aplicație preia starea dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Fiecare aplicație preia datele consumabile ale dispozitivului de imprimare din întreaga flotă prin SNMP
		Intern	Fiecare aplicație poate reporni un dispozitiv de imprimare prin SNMP sau prin interfața de utilizare web a dispozitivului de imprimare
		Intern	Fiecare aplicație poate trimite o pagină de test unui anumit dispozitiv de imprimare
		Intern	Fiecare aplicație poate lansa pagina web a unui dispozitiv de imprimare
		Extern (doar pentru ieșire)	Fiecare aplicație traversează firewall-ul companiei pentru a accesa Internetul (HTTPS prin portul 443)
		Extern (doar pentru ieșire)	Fiecare aplicație se autentifică cu certificatul său de la distanță la serverul de comunicații Xerox înainte de a transmite orice atribut de date
		Extern (doar pentru ieșire)	Fiecare aplicație transmite automat datele despre atributele dispozitivului de imprimare printr-un canal criptat (HTTPS prin portul 443) către Xerox® Communication Servers la o anumită oră în fiecare zi
		Extern (doar pentru ieșire)	Fiecare aplicație interoghează automat serverele Xerox® Communication printr-un canal criptat (HTTPS prin portul 443) la o anumită oră în fiecare zi pentru o listă de acțiuni de efectuat
		Intern	Fiecare aplicație Xerox Device Agent detectează un server proxy web (automat sau direcționat către o anumită adresă)
		Intern	Fiecare aplicație Xerox Device Agent preia capabilitățile dispozitivului de imprimare din întreaga flotă prin SNMP

Metodă de implementare	Aplicație utilizată	Flux de date în rețea	Operabilitate impusă unei rețele
Aplicații de gestionare a dispozitivelor	Ediția pentru parteneri Xerox Device Agent pentru monitorizarea dispozitivelor de imprimare conectate la rețea	Intern	Fiecare aplicație Xerox® Device Agent preia configurația dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Fiecare aplicație Xerox Device Agent preia starea dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Fiecare aplicație Xerox Device Agent preia datele consumabile ale dispozitivului de imprimare din întreaga flotă prin SNMP
		Intern	Fiecare aplicație Xerox Device Agent poate solicita ca dispozitivul să imprime un raport de configurare
		Intern	Fiecare aplicație Xerox Device Agent poate lansa pagina web a unui dispozitiv de imprimare
		Intern	Fiecare aplicație Xerox Device Agent poate actualiza software-ul dispozitivului de imprimare prin trimiterea lucrărilor de imprimare. (. Fișier DLM peste portul 9100)
		Extern (**doar pentru ieșire)**	Fiecare aplicație Xerox Device Agent traversează firewall-ul companiei pentru a accesa Internetul (HTTPS prin portul 443)
		Extern **(doar pentru ieșire)**	Fiecare aplicație se autentifică cu certificatul său de la distanță la serverul de comunicații Xerox înainte de a transmite orice atribut de date
		Extern **(doar pentru ieșire)**	Fiecare aplicație Xerox Device Agent transmite automat datele despre atributele dispozitivului de imprimare printr-un canal criptat (HTTPS prin portul 443) către serverele Xerox® Communication la o anumită oră în fiecare zi
		Extern **(doar pentru ieșire)**	Fiecare aplicație Xerox Device Agent interogează automat serverele de comunicație printr-un canal criptat (HTTPS prin portul 443) la o anumită oră în fiecare zi pentru o listă de acțiuni de efectuat
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent detectează un server proxy web (automat sau direcționat către o anumită adresă)
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent preiau capabilitățile dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent preiau capabilitățile dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent preiau starea dispozitivului de imprimare în întreaga flotă prin SNMP
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent preiau datele despre consumabilele dispozitivului de imprimare din întreaga flotă prin SNMP
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent pot solicita ca dispozitivul să imprime un raport de configurare
		Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent pot lansa pagina web a unui dispozitiv de imprimare

Metodă de implementare	Aplicație utilizată	Flux de date în rețea	Operabilitate impusă unei rețele
Aplicații de gestionare a dispozitivelor	Xerox® Device Manager pentru monitorizarea dispozitivelor de imprimare conectate la rețea	Intern	Aplicațiile Xerox Device Manager / Xerox Device Agent pot actualiza software-ul dispozitivului de imprimare prin trimiterea lucrărilor de imprimare
		Intern	Aplicația Xerox Device Manager acceptă comunicații SNMPv3 cu dispozitive de imprimare
		Intern	Aplicația Xerox Device Manager poate face modificări la configurația dispozitivului de imprimare prin SNMP și interfața de utilizare web
		Intern	Aplicația Xerox Device Manger preia jurnalele de contabilitate bazate pe lucrări de la anumite echipamente multifuncționale Xerox®
		Intern	Aplicația Xerox Device Manager gestionează / impune politicile de control al imprimării
		Extern **(doar pentru ieșire)**	Aplicațiile Xerox Device Manager / Xerox Device Agent traversează firewall-ul companiei pentru a accesa Internetul (HTTPS prin portul 443)
		Extern **(doar pentru ieșire)**	Fiecare aplicație se autentifică cu certificatul său la serverul de comunicații Xerox de la distanță înainte de a transmite orice atribut de date
		Extern **(doar pentru ieșire)**	Aplicațiile Xerox Device Manager / Xerox Device Agent transmit automat datele dispozitivului de imprimare către serverele de comunicații Xerox® printr-un canal criptat (HTTPS prin portul 443) la o anumită oră în fiecare zi
		Extern **(doar pentru ieșire)**	Aplicațiile Xerox Device Manager / Xerox Device Agent interoghează automat serverele de comunicații Xerox printr-un canal criptat (HTTPS prin portul 443) la o anumită oră în fiecare zi pentru o listă de acțiuni de efectuat
	Aplicație de gestionare a dispozitivelor	Extern, bidirecțional	Xerox Device Manager contactează Xerox Services Manager zilnic și permite administratorilor să modifice setările de la distanță, evitând necesitatea serviciilor de întreținere la fața locului.

9. Elemente de securitate

PROTOCOL SIMPLU DE GESTIONARE A REȚELEI (SNMP) PENTRU XEROX®

Protocolul simplu de gestionare a rețelei (SNMP) este cel mai utilizat instrument de gestionare a rețelei pentru comunicarea între sistemele de management al rețelei și imprimantele din rețea. Aplicațiile de gestionare a dispozitivelor utilizează SNMP în timpul operațiunilor de descoperire pentru a prelua informații detaliate despre dispozitivul de imprimare. Aplicațiile de gestionare a dispozitivelor Xerox® acceptă protocoalele SNMP v1/v2 și v3. Consultați ghidurile corespunzătoare de certificare ale aplicației de gestionare a dispozitivelorXerox® pentru detalii specifice.

Cadrul SNMP v3 acceptă mai multe modele de securitate, care pot exista simultan într-o entitate SNMP. SNMPv3 include o securitate mai strictă prin adăugarea de securitate criptografică la SNMPv2. În plus, SNMPv3 este compatibil cu versiunile anterioare și este utilizat pe scară largă în rețelele robuste.

Aplicațiile Xerox Device Management (Centre Ware® Web / Xerox Device Manager, Xerox Device Agent) pot comunica cu platforme de dispozitive care sunt compatibile cu standardul federal de procesare a informațiilor FIPS 140-2 în implementările lor SNMPv3.

Aplicațiile Xerox Device Management nu utilizează serviciul Windows SNMP sau serviciul Windows SNMP Trap. Dacă au fost instalate anterior, aceste servicii **trebuie** să fie dezactivate pe orice computer personal (PC) sau server pe care este instalată aplicația Xerox Device Management.

Aplicațiile Xerox Device Management utilizează un agent SNMP dezvoltat de Xerox care:

- conține un mecanism special de codare/decodare
- este în totalitate gestionat de .NET
- utilizează executabilul de rulare .NET - aceasta oferă securitate sporită pentru a preveni atacurile împotriva vulnerabilităților software-ului, cum ar fi manipulările invalide ale pointerului, depășirile de buffer și verificarea legăturilor.

Aplicațiile Xerox Device Management utilizează caracteristicile de securitate disponibile din sistemul de operare (OS) Windows, inclusiv:

- Autentificarea și autorizarea utilizatorului
- Configurare si management servicii
- Implementarea și managementul politicilor de grup

Internet Connection Firewall (ICF) pentru Windows, inclusiv:

- Setări de securitate la înregistrare
- Setări ICMP

Aplicații de gestionare a dispozitivelor: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, aplicația SQL CE Microsoft® SQL Server și **Xerox Device Manager** utilizează Microsoft® SQL Server.

Aplicațiile Xerox Device Management pot fi configurate pentru a utiliza funcțiile de securitate suplimentare Microsoft® pentru a include, acolo unde este cazul:

- Activarea înregistrării contului de utilizator
- Criptarea sistemului de nume de domeniu (DNS)
- Limitarea privilegiilor contului de utilizator pentru a accesa baza de date (adică drepturile proprietarului bazei de date)
- Punerea în aplicare a unui număr de port definit de utilizator

O cheie de înregistrare Xerox și un cont Xerox valid sunt necesare pentru a transmite date către serverele Xerox de comunicații aflate la distanță.

Aplicațiile Xerox de gestionare a dispozitivelor pot fi afectate de Windows Internet Connection Firewall. (Recomandăm clienților să înscrie URL-ul Xerox pe paravanul de protecție al clientului (*.support.xerox.com) și să specifice adresa IP care poate accesa adresa URL.)

Aplicațiile Xerox Device Management rulează ca proces de fundal folosind acreditările contului de sistem local pentru a interoga automat dispozitivele de imprimare din rețea prin SNMP și pentru a transmite periodic atributele dispozitivului de imprimare înapoi către serverele de comunicații Xerox.

Accesul la interfața de utilizator (UI) și la caracteristicile aplicației Xerox Device Manager este controlat prin următoarele privilegii bazate pe roluri:

- Grupurile Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators și Centre Ware® Web Customers.
- Numele de utilizator și parolele pentru aplicații nu traversează rețeaua; jetoanele de acces sunt utilizate în schimb (prin proiectarea sistemului de operare Windows®).
- Aplicația Xerox Device Manager oferă securitate asupra controlului solicitării tipăririi prin restricționarea sarcinilor în funcție de politica de utilizare a culorii, tipul documentului, costul lucrării, ora din zi, controlul accesului grupului de utilizatori, politica duplex, afișările sarcinilor permise și cotele de imprimare.

Notă: Utilizarea SNMP de către orice aplicație Xerox® Remote Services nu prezintă un risc de securitate pentru mediul IT al unui client, deoarece tot traficul bazat pe SNMP generat sau consumat de aceste aplicații are loc în intranetul clientului, protejat de firewall. Serviciul Windows SNMP și serviciul Windows SNMP Trap nu sunt activate în sistemul de operare Windows în mod implicit.

Modul de securitate al corporației

Sincronizarea ***programată*** de către aplicația Xerox Device Agent cu serverul de comunicații securizate este setată *zilnic*, în mod implicit. Rețineți că ora din zi poate fi setată la o oră aleasă.

Există două tipuri de securitate corporativă: **Normal** și **Blocat.**

Atunci când este setată pe modul **Normal**, aplicaţia de gestionare a dispozitivelor contactează zilnic Xerox Services Manager. Setările pot fi modificate fără a fi nevoie de vizite la fața locului, chiar și atunci când programele de interogare sunt dezactivate. ***(Modul recomandat***).

În modul **Blocat**, în afară de sincronizarea datelor legate de imprimantă, nu există nicio comunicare cu serverele de comunicații, iar setările trebuie modificate la fața locului. În plus, adresele IP ale aparatului Xerox Device Agent și ale imprimantei nu sunt raportate serverului de comunicații. Acest mod limitează toate celelalte beneficii ale serviciilor de la distanță care includ facturarea automată și furnizarea de consumabile, precum și datele de diagnosticare utilizate pentru suport tehnic.

Notă: Dacă o versiune Xerox Device Agent nu conține tab-ul Corporation Security Mode, aceasta funcționează în modul Normal.

10. Impactul asupra rețelei

Regulile de rețea ale companiei vor activa sau dezactiva, de obicei, anumite porturi de rețea pe routere și/sau servere. Majoritatea departamentelor IT sunt preocupate de porturile folosite de aplicație pentru traficul de ieșire. Dezactivarea anumitor porturi poate afecta funcționalitatea aplicației. Consultați tabelul de mai jos pentru porturile specifice utilizate de procesele aplicației. Dacă aplicația trebuie să scaneze pe mai multe segmente de rețea sau subrețele, routerele trebuie să permită protocoalele asociate cu aceste numere de porturi.

Protocoale, porturi și alte tehnologii conexe

Tabelul 7 Identifică protocoalele, porturile și tehnologiile utilizate în Xerox® Remote Services:

Numărul portului	Protocolul	Descrierea utilizării	Fluxul de date în rețea
Depinde de protocoalele de nivel superior	**Protocol Internet (IP)**	**Transport de bază pentru toate comunicațiile de date**	**Intern + Extern (doar pentru ieșire)**
NA	Internet Control Message Protocol (ICMP)	Descoperirea dispozitivului de imprimare + depanare	Intern
25	Simple Mail Transport Protocol (SMTP)	Dispozitiv de imprimare + Alerte de notificare prin e-mail Aplicație Remote Proxy	Intern
53	Domain Name Services (DNS)	Utilizat pentru operaţiunile de descoperire a dispozitivelor de imprimare bazate pe DNS	Intern
80	Hyper Text Transport Protocol (HTTP)	Interogări pagini web pe dispozitivul de imprimare + interogări pagini web în aplicația de gestionare a dispozitivului	Intern
135	Remote Procedure Call (RPC)	Descoperirea dispozitivului de imprimare	Intern
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Protocolul standard din industrie utilizat pentru a descoperi dispozitivele de imprimare în rețea + Preluarea datelor privind starea, contoarele și consumabilele + Preluarea și implementarea configurației dispozitivului de imprimare. Nume implicite ale comunității = „public” (GET), „privat” (SET)	Intern

Numărul portului	Protocolul	Descrierea utilizării	Fluxul de date în rețea
443	Hyper Text Transport Protocol Secure (HTTPS)	Imprimați rezultatele interogărilor securizate în paginile web ale dispozitivului (dacă sunt configurate) + Interogări securizate pentru paginile web ale aplicației Remote Proxy (dacă sunt configurate) + Transferul datelor dispozitivului de imprimare înapoi la Xerox® Communication Servers + comunicațiile de control de tipărire înapoi la Xerox® Device Manager	Intern + Extern (doar pentru ieșire)
515, 9100, 2000, 2105	Trimiterea lucrării de imprimare TCP/IP LPR și Raw Port	Upgrade software pentru dispozitivul de imprimare + Diagnosticare pagină cu Print Test	Intern

11. Cele mai bune practici de securitate

- Țineți întotdeauna dispozitivele de imprimare actualizate la zi cu cel mai recent firmware/ software. Xerox monitorizează îndeaproape vulnerabilitățile și oferă clienților în mod proactiv corecții și actualizări de securitate, atunci când este necesar.
- Dezactivați porturile și protocoalele neutilizate de pe dispozitivele de imprimare ori de câte ori este posibil. Acest lucru se face în mod obișnuit la interfața cu utilizatorul web (UI) a dispozitivelor de imprimare din clasa de birou și la interfața cu utilizatorul local (UI) a dispozitivelor de imprimare din clasa de producție.
- Utilizați funcțiile legate de controlul accesului utilizatorilor pe dispozitivele de imprimare, dacă sunt disponibile. Acest lucru se face în mod obișnuit la interfața cu utilizatorul web (UI) a dispozitivelor de imprimare din clasa de birou și la interfața cu utilizatorul local (UI) a dispozitivelor de imprimare din clasa de producție.
- Utilizați protocoale securizate atunci când este posibil. Acest lucru se face în mod obișnuit la interfața cu utilizatorul web (UI) a dispozitivelor de imprimare din clasa de birou și la interfața cu utilizatorul local (UI) a dispozitivelor de imprimare din clasa de producție.
- Activați funcțiile de securitate încorporate în dispozitiv (de exemplu, suprascrierea imaginii, criptarea datelor scanate, criptarea fluxului de imprimare, criptarea discului, imprimarea securizată, .pdf criptat, autentificarea accesului CAC/PIV.)

Pentru a găsi informații suplimentare despre serviciile la distanță de la Xerox, vizitați Xerox.com/RemoteServices.

Pentru informații suplimentare și specifice cu privire la mecanismele și capabilitățile de securitate din gama de aplicații Xerox Device Management, consultați ghidurile corespunzătoare:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Fie că este vorba despre securitatea dispozitivelor sau a conținutului, Xerox se află în prima linie a luptei de combatere a amenințărilor emergente de astăzi prin politicile sale proactive de securitate. Vizitați www.xerox.com/security pentru a accesa o gamă completă de informații de securitate, actualizări, buletine, cărți albe, corecții și multe altele.