Remote Services @ Xerox

Sikkerhedshvidbog

Version 4.0

Marts 2022

Dette dokument ændres fra tid til anden. Ændringer, tekniske unøjagtigheder og typografiske fejl vil blive rettet i efterfølgende udgaver.

IS 614672/IS 514590

Indholdsfortegnelse

1. Overordnet formål og publikum

Sikkerhedshvidbogen til Remote Services @ Xerox har til formål at hjælpe kunder med at forstå og implementere den sikre fjernserviceløsning, som fungerer bedst med deres netværkskonstruktion og informationssikkerhedspolitikker. Med henblik på at skabe den mest sikre konfigurationsmetode skal det bemærkes, at ændringer af kundens internet-firewall, webproxy-servere eller anden sikkerhedsrelateret netværksinfrastruktur kan være påkrævet.

Målgruppen for dette dokument omfatter tekniske leverandører, netværksadministratorer og fagfolk inden for netværkssikkerhed, der er interesserede i fjerntjenesternes muligheder såvel som sikkerhedsimplementeringen af disse funktioner.

Vi anbefaler, at dokumentet gennemlæses i sin helhed med henblik på at certificere brugen af Xerox®'s produkter og tjenesteydelser inden for kundens netværksmiljø.

2. Værdiforslag

Vi tilbyder en sikker og sikker måde, hvorpå enhedsdata sendes til vores ISO-certificerede system for at automatisere almindelige opgaver og levere en bedre service- og supportoplevelse.

- Afregningsmålerrapportering er automatiseret og nøjagtig.
- Automatisk genopfyldningsprogram for forbrugsvarer leverer toner på baggrund af printerens indrapporterede tonerniveauer, så der ikke er behov for at spore lagerbeholdning eller ringe efter forbrugsvarer.
- Sending af diagnosticeringsoplysninger giver os mulighed for bedre at understøtte din enhed, hvilket ofte muliggør hurtigere problemløsning.
- Visse printermodeller kan søge efter vigtige softwareopdateringer og installere opdateringerne programmatisk uden kundeintervention.[Se bemærkning]
- Vores løsninger til administration giver også mulighed for at administrere printere, der ikke kommer fra Xerox.
- Disse tjenester lader vores kunder udnytte tiden mere effektivt.

Alt dettes gøres med sikkerhed i tankerne.

Bemærk: Denne mulighed kan deaktiveres for miljøer, hvor kunder certificeres til en bestemt softwareversion og ønsker at kontrollere udskrivningssoftwaren, når der oprettes opdateringer. Dette kan gøres uden at deaktivere de øvrige remote services-funktioner.

3. Remote services

Information er et nøgleaktiv, og sikkerhed er altafgørende for alle organisatoriske aktiver, herunder netværksforbundne multifunktionsudskrivningsenheder (MFP'er). I dag indebærer det at administrere en flåde af multifunktionsudskrivningsenheder og samtidig sikre et acceptabelt sikkerhedsniveau en række unikke udfordringer, som ofte overses. Vi forstår denne kompleksitet og er lydhør over for vores kunders sikkerhedsbehov. Xerox®-produkter, Xerox®-systemer og fjerntjenester er designet til sikker integration med vores kunders eksisterende arbejdsgange, alt imens de anvender de nyeste sikre teknologier.

Som standard sendes ingen kundebilleder fra udskrivning, fax, scanning, kopihandlinger eller andre følsomme oplysninger til vores servere.

De amerikanske Xerox-servere overholder strenge sikkerhedskrav til sikkerhedsadministration af information. Vores datacentre og apps til remote services opretholder den årlige Statement on Standards for Attestation (SSAE) No-16, overensstemmelseskrav Sarbanes-Oxley Act (SOX), og er ISO 27001:2013-certificeret.

4. Implementeringsmodeller

Kunder kan vælge mellem følgende lige sikre Xerox® remote services-implementeringsmodeller:

- **Kombinationmsodel** – ***(foretrukken model)*** Implementeringen af app-modellen Device Direct og Device Management er en ideel kombination, eftersom den leverer de mest robuste datasæt og enhedsadministrationsfunktioner.

- **Model med Device Direct** – Device Direct gør det muligt for udskrivningsenheder at kommunikere direkte til de eksterne Xerox®-kommunikationsservere via internettet igennem kundens firewall med henblik på at understøtte Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) såvel som enhedsdiagnoserapportering. Denne implementeringsmodel omfatter et sæt dataelementer i standardnyttelasten, der inkluderer enhedsfejl, advarsler, tællere, HFSI (High Frequency Service Items) og andre egenskaber for udskrivningsenheder.
- **Model med Device Management Application** – apps af typen Xerox® kan implementeres i en kundes netværk med henblik på at indsamle et sæt dataegenskaber fra udskrivningsenheder og ligeledes understøtte Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) såvel som enhedsdiagnoserapportering. Egenskaber for udskrivningsenheder indsamles og overføres efterfølgende sikkert til Xerox's fjernservere. Dataegenskaber fra både Xerox- og ikke-Xerox-udskrivningsenheder kan kommunikeres som en del af denne implementeringsmodel.

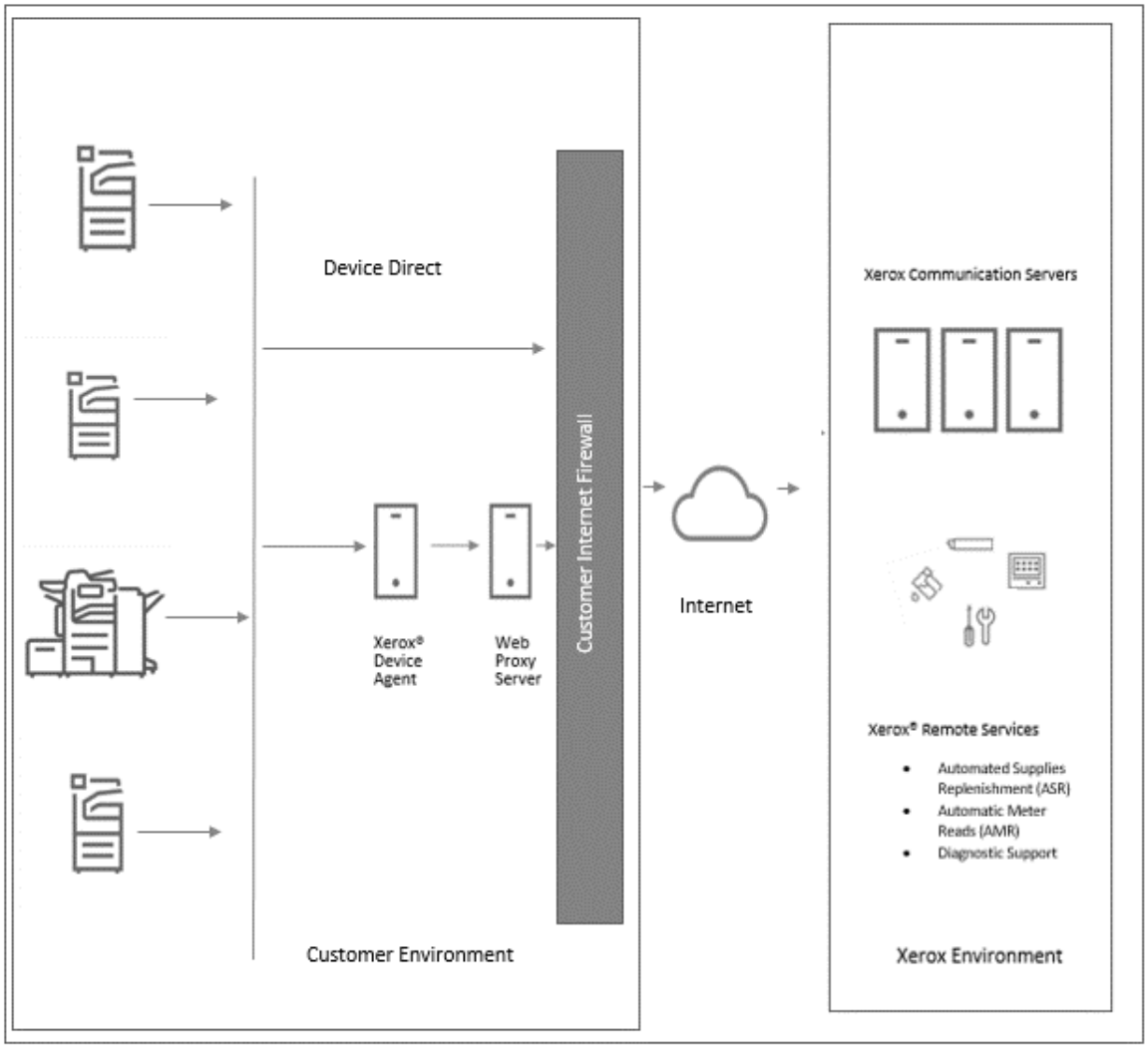
Alle implementeringsmodeller for Xerox® Remote Services er lige sikre og udnytter de nyeste branchestandarder, webbaserede protokoller og porte til at oprette en sikker, krypteret kanal, når der overføres printenhedsegenskaber eksternt til de eksterne Xerox-servere, der er placeret i vores redundante sikrede datacentre.

Den valgte implementeringsmodel afhænger af vores kunders type printserviceløsning, informationssikkerhedspolitikker og regler for håndtering af transmissionen af printenhedens dataegenskaber.

Kombineret udviklingsmodel (foretrukken)

Kombinationsimplementeringen implementeres, når en kunde køber flere typer Xerox-vedligeholdelsesaftaler til deres udskrivningsenheder med henblik på at opnå en mere robust fjernserviceløsning. Når en Xerox®-udskrivningsenhed første gang installeres på et netværk, sikrer Xerox's remote services-standardadfærd, at printerenheden automatisk forsøger at kommunikere udgående til vores kommunikationsservere ved hjælp af en sikker, godkendt forbindelsesmetode.

Figur 1



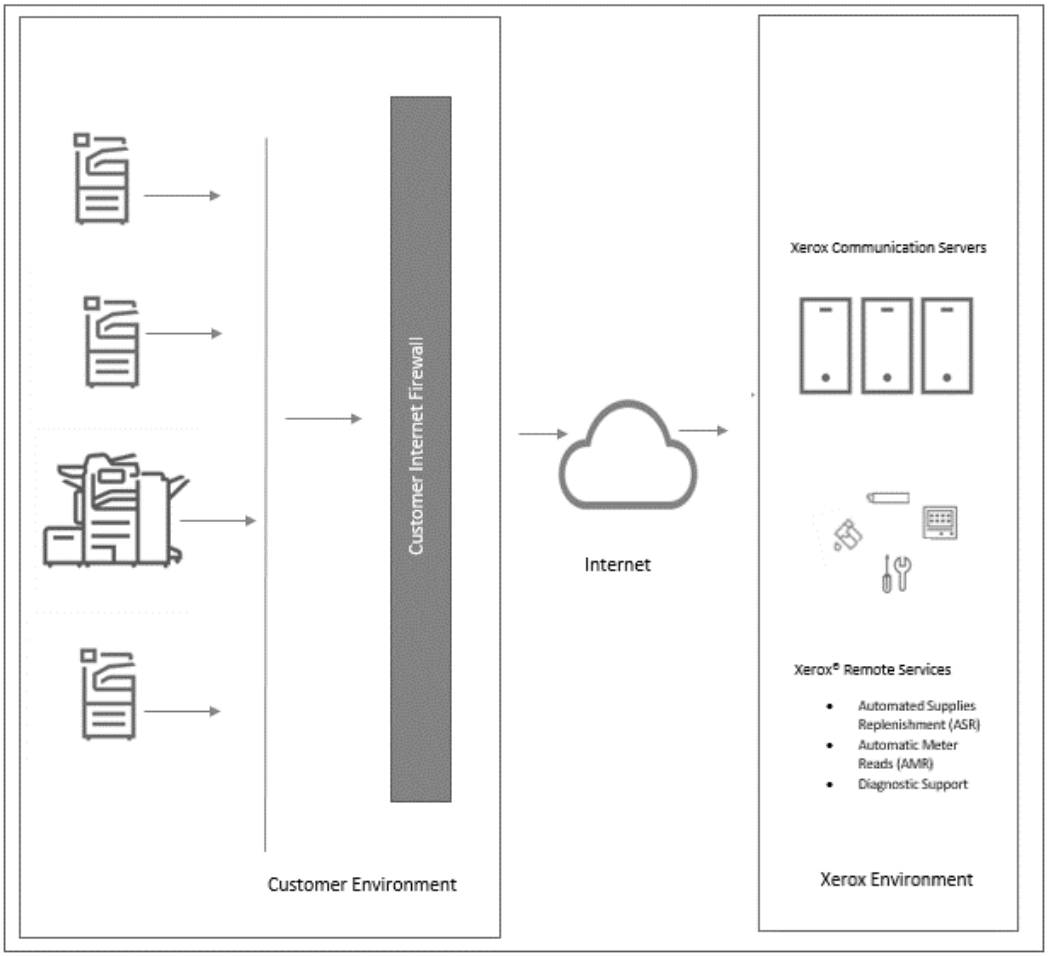
Combination Deployment Model

Model med Device Direct Deployment

Xerox®-enheder, der er kompatible med remote services, anvender en protokolforbindelse af typen Transport Layer Security (TLS) 1.2 over den sikre standardport 443 til udgående kommunikation med vores sikre servere.

- Udskrivningsenheder inden for kundemiljøet indleder al kommunikation med kommunikationsserverne. Normale firewall-konfigurationer på webstedet er påkrævet for at aktivere kommunikation.
- Der skal bruges en URL (*.xerox.support.com) til kommunikationsservere med henblik på at godkende udskrivningsenheder til Xerox's infrastruktur
- Enheden anmoder om en registrering hos kommunikationsserverne ved hjælp af de relevante legitimationsoplysninger for certifikatgodkendelse.
- Kommunikationsserverne validerer de legitimationsoplysninger, som printerne har leveret, og accepterer anmodningerne.
- Kommunikationsserverne befinder sig bag en sikker firewall og er ikke tilgængelige fra internettet.

Figur 2



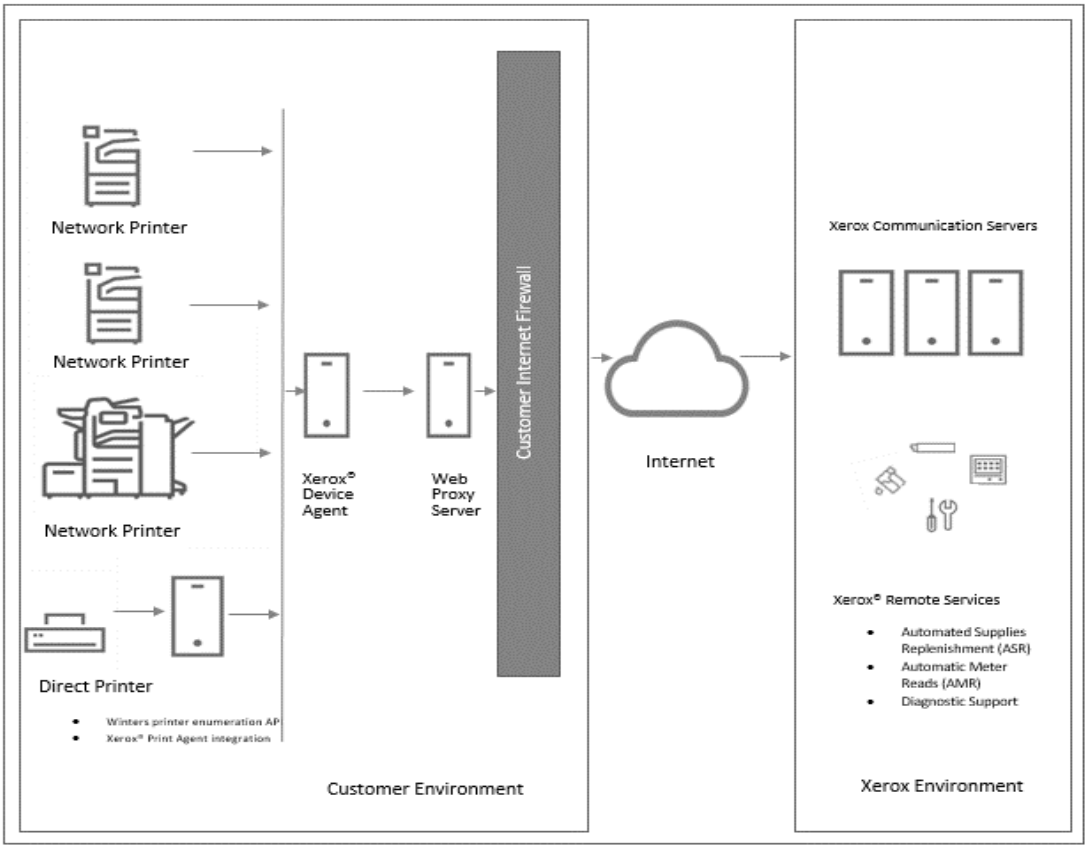
Device Direct Deployment Model

Model med Device Management Application Deployment

Device Management Applications (dvs. **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **og Xerox Device Manager)** anvender en protokol af typen Transport Layer Security (TLS) 1.2 til at kommunikere eksternt med kommunikationsserverne. Yderligere funktioner udnyttes til at forbedre sikkerheden på tværs af denne kanal og oprettes under den indledende installation af apps af typen Device Management, som omfatter:

- Appen Device Management i kundemiljøet indleder al kommunikation med kommunikationsserverne. Normale firewall-konfigurationer på webstedet er påkrævet for at aktivere kommunikation.
- Kommunikationsserverne befinder sig bag en sikker firewall og er ikke tilgængelige fra internettet.
- Appen Device Management anmoder om en registrering hos fjernserverne ved hjælp af certifikatgodkendelse passende legitimationsoplysninger.
- Kommunikationsserverne validerer de legitimationsoplysninger, som printerne har leveret, og accepterer anmodningerne.
- Appen Device Management godkender kommunikationsserverne og aktiverer tjenesten.

Figur 3



Device Management Application Deployment Model

5. Dataoverførsel og nyttebelastning

Datakilder

Udskriftsenhedens dataegenskaber, der sendes som en del af den overførte nyttebelastning, er fra følgende kilder:

- Xerox® Office-netværksprintere
- Ikke-Xerox-netværksprintere
- Xerox®-produktionsprintere
- Apps af typen Xerox® Device Management

Bemærk: Ikke alle Xerox-printere til kontor- og produktionsbrug er kompatible med Xerox Remote Services. Du finder en komplet liste over kompatible produkter her. Udskrivningsegenskaberne afhænger af produktet og implementeringsløsningen tilhørende Xerox® Remote Services.

Xerox®-enheder til kontorbrug

Tabel 1 identificerer de enhedsdataegenskaber, der kan overføres til remote serivces, som er kompatible med Xerox®'s kontorprodukter

Dataegenskaber	Detaljeret beskrivelse af dataegenskaber
Udskrivningsenhedens identitet	Inkluderer model, modulfirmwareniveauer, modulserienumre, modulinstallationsdatoer, licensdata og placering, hvis tilgængelig.
Udskrivningsenhedens netværksadresse	Omfatter Media Access Control-adresse (MAC), undernettets adresse.
Udskrivningsenhedens egenskaber	Inkluderer detaljeret hardwarekomponentkonfiguration, detaljeret softwaremodulkonfiguration, understøttede funktioner/tjenester osv.
Status for udskrivningsenhed	Omfatter aktive statusser, optællinger af fejlhistorik, DFE-begivenhedslog, datatransmissionshistorik
Udskrivningsenhedstællere	Omfatter faktureringsmålere, udskrivningsrelaterede tællere, kopirelaterede tællere, tællere relateret til større job, produktionsspecifikke tællere, scan til destination-relaterede tællere på prisbillige produktionsmodeller osv.
Udskrivningsenheders forbrugsstoffer	Omfatter producent, model, serienummer, navn, type, niveau, kapacitet, status, levetidstællere osv.
Udskriv detaljerede oplysninger om maskinbrug	Omfatter HFSI-data, NVM-data, udskiftning af dele, DFE-logfiler, detaljerede diagnostiske data, fejlløsning.
Teknik/fejlfinding	Omfatter ikke-strukturerede, detaljerede fejlretningsrelaterede data, som kun er beregnet til support på tredje niveau.

Dataegenskaber	Detaljeret beskrivelse af dataegenskaber
Kundejobrela-teret	Xerox® Production-udskrivningsprodukter gør det muligt at reproducere jobrelaterede data til støtte for eskalerede supportscenarier via krypteret PostScript til Xerox. Kunden kan kontrollere, om denne funktion skal aktiveres eller ej. Hvis kunden vælger at overføre jobrelaterede data (dvs. krypteret PostScript) tilbage til Xerox, håndteres disse data i overensstemmelse med Xerox's politikker og standarder for informationssikkerhed (IS).

Vores udskrivningsenheder i kontorklassen transmitterer enhedsdataegenskaberne i et XML-format (eXtensible Markup Language) ved hjælp af en komprimeret .zip-fil. Efter godkendelse overføres hver enkelt fil derefter med en krypteret kanal til kommunikationsserverne.

Xerox®-enheder til produktionsbrug

Tabel 2 identificerer de enhedsdataegenskaber, der kan overføres til remote serivces, som er kompatible med Xerox®'s produktionsprodukter

	Beskrivelse
Udskrivningsen-hedens identitet	Omfatter model, firmwareniveau, modulserienumre og installationsdato.
Udskrivningsen-hedens netværksadresse	Omfatter Media Access Control-adresse (MAC), undernettets adresse.
Udskrivningsen-hedens egenskaber	Inkluderer detaljeret hardwarekomponentkonfiguration, detaljeret softwaremodulkonfiguration, understøttede funktioner/tjenester, strømsparetilstande osv.
Status for udskrivningsenhed	Indeholder overordnet status, detaljerede advarsler, historik over de seneste 40 fejl, fastklemningsdata osv.
Udskrivningsenheds-tællere	Omfatter faktureringsmålere, udskrivningsrelaterede tællere, kopirelaterede tællere, faxrelaterede tællere, tællere relateret til større job, scan til destination-relaterede tællere, brugsstatistikker osv.
Udskrivningsen-heders forbrugsstoffer	Indeholder navn på forbrugsvarer, type (f.eks. billedbehandling, efterbehandling, papirmedier), niveau, kapacitet, status, størrelse osv.
Udskriv detaljerede oplysninger om maskinbrug	Inkluderer detaljerede udskrivningsrelaterede tællere, opstartstilstande, detaljerede udskiftningsmængder af Customer Replaceable Units (CRU), detaljerede CRU-fejldata og distributioner, indlejret OCR-funktionalitet (Optical Character Recognition), fordeling af udskriftslængde, distribution af papirbakkebrug, medier installeret, medietypefordeling, mediestørrelsesfordeling, dokumentlængdefordeling, sætnummer, HFSI-data, NVM-data, distribution, markerede pixelantal, gennemsnitlig områdedækning pr. farve, fejl/stop, detaljerede scanningsrelaterede tællere
Teknik/fejlfinding	Omfatter detaljerede fejlfindingsoplysninger, der kan inkludere data uden for datasættet ovenfor. Disse data kan omfatte PII såsom brugernavne, e-mail-adresser og jobdata. Disse data sendes kun med udtrykkelig tilladelse fra kunden og er kun beregnet til eskaleret fejlfinding supportbrug.

Vores udskrivningsenheder i produktionsklassen transmitterer enhedsdataegenskaberne i et XML-format (eXtensible Markup Language) ved hjælp af en komprimeret .zip-fil. Efter godkendelse overføres hver enkelt fil derefter med en krypteret kanal til remote service-servere.

Bemærk: Filen og indholdet af de identificerede data varierer afhængigt af produktmodel.

Apps af typen Xerox® Device Management

Der er adskillige apps af typen Device Management tilgængelige på baggrund af kundens netværksmiljø og behov for administration af udskrivningsenheder. Hver enkelt er lige sikre og har robuste funktioner til enhedsadministration.

Følgende er en liste over apps til enhedsadministration: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition og Xerox Device Manager.

Hvert enkelt program synkroniserer som standard med sikre kommunikationsservere én gang i døgnet som minimum. Med henblik på at skabe optimal sikkerhed for dine data er kommunikationsserverne hostet i et ISO 27001-kompatibelt anlæg. Data, der sendes, er primært printerspecifikke faktureringstællere, forsyningsniveauer og printeradvarsler. Data komprimeres, krypteres og beskyttes af flere mekanismer:

- Appen Xerox Device Management starter al kontakt med Xerox's kommunikationsservere, standard firewall-konfigurationer i kundemiljø er påkrævet for at aktivere kommunikation.
- Apps af typen Xerox Device Management kræver en gyldig proxy, hvis der er behov for en proxy til internetkommunikation.
- Xerox' kommunikationsservere er placeret bag en sikker firewall i Xerox-miljøet og er ikke tilgængelige fra internettet.
- Xerox's kommunikationsservers brugergrænsefladeadgang kræver godkendelse. Appen Xerox Device Management-værtsoplysninger gemmes på en konto, der er specifik for kundens websted, og adgangen til disse kontodata på Xerox-kommunikationsservere er begrænset til Xerox-kommunikationsserverens kontoadministratorer.
- Al Xerox’s kommunikationsservers kommunikation logges og er tilgængelig til visning.
- Data, der sendes til dine netværksudskrivningsenheder, når de er aktiveret, består primært af fjernkommandoer, der gør det muligt for en kontosupportadministrator at anmode om gennemførsel af Xerox Device Management-kommandoniveau under eskalerede supportscenarier.
- Forespørgsler involverer primært firmwareopdateringer, genstart af printer, udskrivning af testside og opdatering af den aktuelle enhedsstatus.
- Appen Xerox Device Management anmoder periodisk dens Xerox-kommunikationsserverkonto om kommandoanmodninger.
- Operationsresultater fra kommandoanmodninger sendes til Xerox’s kommunikationsservere, hvor de derefter gennemgås.

Bemærk: Der er et krav om engangsregistrering ved softwareinstallation. Disse registreringsoplysninger Indeholder et felt til enhedens placering og e-mail til kontakt.

Apps af typen Xerox Device Management **(dvs. Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition og Xerox Device Manager** transmitterer udskrivningsegenskaberne i et XML-format (eXtensible Markup Language) ved hjælp af en komprimeret .zip-fil. Filen bliver derefter krypteret og transmitteres via krypterede kanaler til fjernkommunikationsservere.

Tabel 3 Identificerer en liste over enhedens dataegenskaber samt en beskrivelse, der kan sendes via appen Xerox® Device Mgmt.

Dataegenskaber	Detaljeret beskrivelse af dataegenskaber
Udskrivningsenhedens identitet	Inkluderer producent, model, beskrivelse, firmwareniveau, serienummer, aktiv-tags, systemnavn, kontaktperson, placering, administrationstilstand for arbejdsstation (desktop), faxtelefonnummer og kønavn.
Udskrivningsenhedens netværksadresse	Inkluderer MAC-adresse, IP-adresse, DNS-navn, undernetmaske, IP-standardgateway, senest kendte IP-adresse, IP-adresse ændret, tidszone, IPX-adresse, IPX-eksternt netværksnummer, IPX-printserver.
Udskrivningsenhedens egenskaber	Inkluderer installerede komponenter, komponentbeskrivelser, understøttede funktioner/tjenester, printhastighed, farveunderstøttelse, efterbehandlingsmuligheder, dupleksunderstøttelse, mærkningsteknologi, harddisk, RAM, sprogunderstøttelse, brugerdefinerede egenskaber.
Status for udskrivningsenhed	Inkluderer overordnet status, detaljerede advarsler, lokale konsolmeddelelser, komponentstatus, statusgenfindingsrelaterede data, opdagelsesdato, opdagelsesmetode/-type, enhedens oppetid, understøttede/aktiverede traps.
Udskrivningsenhedstællere	Omfatter faktureringsmålere, udskrivningsrelaterede tællere, kopirelaterede tællere, faxrelaterede tællere, tællere relateret til større job, scanningsrelaterede tællere, brugsstatistikker og målvolumen.
Udskrivningsenheders forbrugsstoffer	Indeholder navn på forbrugsvarer, type (f.eks. billedbehandling, efterbehandling, papirmedier), niveau, kapacitet, status, størrelse og relaterede egenskaber
Detaljeret brug af udskrivningsenhed	Brugerbaserede jobsporingsdata, som omfatter jobkarakteristika (id, dokumentnavn, ejer, dokumenttype, jobtype, farve, dupleks, påkrævet medie, størrelse, sider, sæt, fejl), destination (printenhed, model, DNS-navn, IP-adresse, MAC-adresse, serienummer), resultater af udskrivning af jobbet (afleveringstid, jobudskrivningstid, udskrevne sider, udskrevne farvesider /sort-hvide sider, anvendt farvetilstand, N-up), regnskabsdata (tilbageførselskode, tilbageførselspris, regnskabskilde), kilde til udskriftsjob (arbejdsstation, printerservernavn/MAC-adresse, kønavn, port, brugernavn, bruger-id), Xerox-administrationsdata (sendt til Xerox Services Manager).
Enhedsstyringsidentitet	Omfatter applikationsværts pc-oplysninger såsom DNS-navn, IP-adresse, OS-navn, OS-type, pc-CPU, RAM-størrelser (fri kontra udnyttet), harddiskstørrelser (fri kontra udnyttet), webstedsnavn, app-version, app-licensudløb dato, .Net-version, tidszone, version af opdagelseskomponent, størrelse på hoveddatabasen, størrelse på opdagelsesdatabase, antal printere/inden for rækkevidde/uden for rækkevidde, kørende kritiske tjenester.
Device Manager Corporation Security Mode	Normal tilstand = Xerox Device Agent kontakter dagligt Xerox Services Manager. Indstillinger kan ændres eksternt uden behov for besøg på stedet, selv når afstemningsplaner er slået fra. Nedlukningstilstand = udover printerrelateret datasynkronisering er der ingen kommunikation med Xerox Services Manager, og indstillingerne skal ændres på stedet. Xerox Device Agent-maskinen og printerens IP-adresser indberettes til Xerox Services Manager.
Kontrolpolitik for undsivning af enhedsadministration	Inkluderer slutbruger pc-navn, benyttet printserver, bemuttet udskriftskø, tidsstempel for overtrædelse, dokumentnavn, slutbrugerbrugernavn, job-duplex, jobfarve, samlede visninger af job, jobpris, udført handling, slutbruger underrettet, meddelelse vist, udskrivning af politiknavn, udskriftspolitikregel.

6. Fjernadministration af udskrivningsenheder

Xerox eskalerede supportpersonale kan behandle følgende handlinger via Device Direct eller appen Xerox Device Management.

Tabel 4 viser forbedrede løsningsbestræbelser, der tillades af kunden i et eskaleret supportscenarie. Kundens tilladelse til at udføre disse funktioner skal indhentes udtrykkeligt.

Data	Beskrivelse
Handlinger, der skal udføres på udskrivningsenheder	• Hent enhedsstatus = hent den seneste status fra udskrivningsenheden • Genstart enhed = start en sluk-/startsekvens på printerenheden • Opgrader enhed = installer software/firmware på udskrivningsenheden (.DLM over port 9100) • Fejlsøg enhed = ping enhed + hent seneste status fra udskrivningsenheden • Udskriv testside = send et testjob til en udskrivningsenhed for at validere udskriftsstien (opretter en konfigurationsrapport) • Start administration af enhed = start periodiske overførsler af udskriftsenhedsdata til de eksterne Xerox®-kommunikationsservere **Bemærk: Hver enkelt handling kan deaktiveres fra brug on demand i administrationskonfigurationsdelen af Xerox® Device Management Applications, der understøtter denne funktion.**
Handlinger, der skal udføres på Device Management Applications	Indstillinger inden for hver enhedsadministrationsapplikation, som kan administreres, omfatter registreringsdrift, dataeksportfrekvens, SNMP-kommunikationsrelaterede indstillinger (genforsøg, timeout, fællesskabsnavne), advarselsprofiler og opdateringsfrekvens for software til automatisk enhedsadministration.
Administration af fjernsoftware	Visse enheder er udstyret med automatiseret fjernsoftwarestyring. Disse enheder sender en forespørgsel til Xerox-miljøet for at afdække, om der er nye softwareopdateringer tilgængelige til enheden. Hvis der er, vil enheden derefter kunne sende en anmodning om den pågældende softwareopdatering, og enheden vil blive opdateret på det forespurgte tidspunkt. Hvis dit miljø forbyder automatiske softwareopdateringer, kan muligheden for fjernstyring af software dog kun fravælges uden afbrydelse af standardfjerntjenester.

Systemkrav til apps apps af typen Device Manager

Minimumskravene afhænger i nogen grad af tilbuddene. Se brugervejledningen, sikkerhedsevalueringsvejledningen og/eller certificeringsvejledningen for at få oplysninger om grundlæggende krav, der er specifikke for de respektive apps til enhedsadministration.

Ved installationen medfølger der en readme-fil med henblik på at imødekomme yderligere og specifikke systemkrav for den respektive enhedsadministrationsapplikation, der installeres.

- Apps af typen Device Management er kompatible med sikkerhedsfunktionerne indbygget i Windows®-operativsystemet. De er afhængige af en Windows®-baggrundstjeneste, der kører under de lokale systemkontolegitimationsoplysninger med henblik på at muliggøre proaktiv overvågning af printere og udskriftsdataattributtens nyttebelastning, der overføres til Xerox. Brugergrænsefladen, der viser udskriftsdataattributtens nyttebelastning, er kun tilgængelig for superbrugere og administratorer med adgang til Windows® OS.

- Med henblik på at forebygge afbrydelse af den automatiske fjerntjenestekommunikation anbefales det, at appen Device Management indlæses på en klient, der er strømforsynet kontinuerligt eller i kernearbejdstiden.

- Vi anbefaler, at værtscomputere kører et understøttet opreativsystem fra Microsoft® Corporation. Apps af typen Xerox Device Management kan dog køres på Apple® OS 10.9.4 eller nyere ved hjælp af emuleringssoftwaren Parallels Desktop. Appen kan ikke køre i et hjemhørende Macintosh-miljø. Se de pågældende brugervejledninger for at få detaljeret support. Der findes oplysninger om krav drift på et Macintosh-operativsystem

- Vi anbefaler, at værtscomputere opdateres med de nyeste vigtige patches og tjenesteudgivelser fra Microsoft® Corporation.

- Network Transmission Control Protocol/Internet Protocol (TCP/IP) skal være indlæst og driftsduelig.

- Der kræves administrative rettigheder til installation af app-softwaren Device Management på klientmaskinen.

- Kræver SNMP-aktiverede enheder og muligheden for at drive SNMP over netværket. Det er ikke nødvendigt at aktivere SNMP på den computer, hvor apps af typen Xerox® Device Management vil blive installeret, eller på andre netværkscomputere.

- Microsoft®.NET Framework skal være installeret før installation af appen.

- Appen bør ikke installeres på en pc, hvor andre SNMP-baserede programmer eller andre Xerox® Print-administrationsværktøjer er installeret, eftersom disse kan forstyrre hinandens drift.

Databasekonfigurationer

- Applikationen installerer databasemotoren SQL Server Compact Edition (SQL CE) og databasefiler, der lagrer printerdata og applikationsindstillinger i installationsmappen. Der er ikke behov for databaselicensering til appen. Xerox® Device Agent understøtter også eksisterende udgaver af SQL Server som beskrevet ovenfor.

Ikke-understøttede konfigurationer

Dette afsnit beskriver de konfigurationer, der ikke er understøttet.

- Installation af programmet på en computer med et andet Xerox-enhedsstyringsprogram som f.eks. Xerox Device Manager.

- Hjemmehørende Mac OS®-operativsystemsoftware (dvs. Xerox Device Agent kan kun køre på platformen Apple Mac, når softwaren Parallels Emulation er installeret.)

- Alle versioner af UNIX®-operativsystemer, operativsystemer fra Linux®, Windows®-systemer, der kører Novell-klienten, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 og 2008 R2, Windows® Server 2003, Windows® 8 RT, operativsystemer, der kører Terminal Services for apps og installation på Windows-systemer, som kører domænecontrollere.

Eftersom dette program alene er blevet testet på VMware® Lab Manager/i et arbejdsstationmiljø, understøttes øvrige virtuelle miljøer ikke.

7. Xerox®'s forretningsproces og tjenesteydelser

De data, der modtages fra Xerox® Office-baserede udskrivningsenheder, Xerox® Production-baserede udskrivningsenheder, samt apps af typen Xerox Device Management som en del af remote services-løsningen anvendes af Xerox-virksomhedsprocesser som anført ovenfor:

Tabel 5 beskriver navnet og beskrivelsen af den forretningsproces og de tjenester, der understøttes som en del af Remote Services-løsningen.

Navn på forretningsproces	Beskrivelse
Automatiske målerudlæsninger	Måleraflæst data bruges i faktureringsprocessen.
Automatisk påfyldning af forsyninger/automatisk levering af reservedele	Toner sendes automatisk til kunder baseret på status for udtømning af forbrugsvarer modtaget fra printenheder. Visse udskiftelige komponenter sendes automatisk til kunderne, når de er nødvendige til deres udskrivningsenheder. Disse muligheder er kun tilgængelige for kunder, der vælger kontrakter med målt levering.
Servicevenlighed (vedligeholdelsesassistent)	Fjernstyring af enheden tilvejebringer detaljerede fejloplysninger, som kan ses af Xerox's servicepersonale, når det er nødvendigt, med henblik på at fremskynde forberedelsen til et besøg på stedet eller diagnosticere og afhjælpe problemer.
Support på tredje niveau (teknik/fejlfinding)	Produktsupportpersonale kan fejlsøge vanskelige problemer, når de får adgang til detaljerede teknik- og fejlretningslogfiler.
Produktudvikling	Data for printerens ydeevne og anvendelsesdata benyttes til at identificere produktforbedringer til fremtidige udgivelser.

Grundlæggende printenhedsdata sammensættes, transmitteres, opbevares og arkiveres i et ISO-27001-certificeret Xerox-datacenter og lagres i overensstemmelse med Xerox-virksomhedens retningslinjer for opbevaring af datahåndtering

De arbejdsprocesser og den arbejdspraksis, der understøtter og beskytter softwaresystemerne til fjerntjenester, er baseret på best practice for ITIL og Xerox's informationssikkerhedspolitikker, som er direkte i overensstemmelse med ISO 27002-standarderne for informationssikkerhedsstyringssystem fra International Standards Organization. Kunder kan være sikre på, at styring, beskyttelse og opbevaring af enhedsdata omfatter de grundlæggende principper for informationssikkerhed: fortrolighed, integritet, tilgængelighed, godkendelse og ikke-afvisning.

8. Teknologiske oplysninger

Dette afsnit indeholder yderligere tekniske detaljer, som typisk kræves af it-teams (IT) og sikkerhedspersonale, der håndterer risici ved at opnå sikkerhed for sikker udviklingspraksis. En sådan forsikring gør dem i stand til at certificere vores udskrivningsenheder og apps af typen Device Management til brug i kundens netværksmiljø.

Softwaredesign

Vores engagement i Xerox's produktsikkerhed begynder tidligt i produktudviklingen, hvor Xerox's udviklere følger en formel sikkerhedsudviklingslivscyklus, der håndterer sikkerhedsproblemer igennem identifikation, analyse, prioritering, kodning og test. Mange Xerox®-udskrivningsenheder er Common Criteria-certificeret iht. ISO IEC 15408 eller er aktivt under certificeringsgennemgang.

Driftsevne

Xerox's remote services gennemfører følgende typer operationer på et netværk. Disse operationer afhænger af den konfigurerede implementeringsmetode.

Tabel 6.

Implementeringsmetode	Anvendt app	Datastrøm på netværket	Driftsevne pålagt et netværk
Device Direct	Ingen	Intern	Xerox®-udskrivningsenheden forsøger at registrere en Web Proxy Server (automatisk eller videresendt til en bestemt adresse)
		Intern	Xerox®-udskrivningsenheder kan programmeres til at oprette anmodninger til en Simple Mail Transport Protocol-server (SMTP) om af afsende e-mail-meddelelser med e-mail-alarmer til en defineret modtagerliste
		Ekstern for netværket	Xerox®-udskrivningsenheden krydser virksomhedens firewall for at få adgang til internettet (HTTPS over port 443)
		Ekstern for netværket	Xerox®-udskrivningsenheden godkendes med dens certifikat Remote Xerox Communication Server, før der transmitteres nogen dataegenskaber
		Ekstern for netværket	Xerox®-udskrivningsenheden transmitterer automatisk udskrivningsenhedens egenskabsdata igennem en krypteret kanal (HTTPS over port 443) til Xerox® Communication Servers på et bestemt tidspunkt på dagen eller på anmodning af kunden.
		Ekstern for netværket	Xerox®-udskrivningsenheden forespørger automatisk Xerox® Communication Servers igennem en krypteret kanal (HTTPS over port 443) om en liste over handlinger, der skal gennemføres (f.eks. afsendelse af faktureringsdata nu, tilføjelse af en tjenesteydelse m.v.), på et bestemt tidspunkt hver dag
		Ekstern for netværket	Envejstransmission on demand af Xerox®-udskrivningsenhedens tekniske logdata igennem en krypteret kanal (HTTPS over port 443) til Xerox® Communication Server

Implementeringsmetode	Anvendt app	Datastrøm på netværket	Driftsevne pålagt et netværk
Device Direct	Ingen	Outbound, initiated by dev to pull latest s/w	Enheden sender forespørgsel til en ekstern softwareadministrationsserver med henblik på at kontrollere for software-/sikkerhedsopdateringer. Hvis kundens miljø forbyder automatiske softwareopdateringer, kan muligheden for fjernstyring af software dog kun fravælges uden afbrydelse af standardfjerntjenester.
Apps til enhedsadministration	Centre Ware® Web	Intern	Hver enkelt app registrerer en webbaseret proxyserver (automatisk eller videresendt til en bestemt adresse)
		Intern	Hver enkelt app henter udskrivningsenhedens funktioner på tværs af flåden via SNMP
		Intern	Hver enkelt app modtager udskrivningsenhedskonfiguration på tværs af flåden via SNMP
		Intern	Hver enkelt app modtager status om udskrivningsenheden på tværs af flåden via SNMP
		Intern	Hver enkelt app modtager forbrugsdata for udskrivningsenheder på tværs af flåden via SNMP
		Intern	Hver enkelt app kan genstarte en udskrivningsenhed via SNMP eller via udskrivningsenhedens webgrænseflade
		Intern	Hver enkelt app kan indsende en testside til en specifik udskrivningsenhed
		Intern	Hver enkelt app kan åbne en udskrivningsenheds webside
		Ekstern **(kun udgående)**	Hver enkelt app krydser virksomhedens firewall for at få adgang til internettet (HTTPS over port 443)
		Ekstern (**kun udgående)**	Hver enkelt app godkendes med dens certifikat Remote Xerox Communication Server, før der transmitteres nogen dataegenskaber
		Ekstern **(kun udgående)**	Hver app transmitterer automatisk udskrivningsenhedens egenskabsdata via en krypteret kanal (HTTPS over port 443) til Xerox®-kommunikationsservere på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Hver enkelt app anmoder automatisk Xerox® Communication Servers igennem en krypteret kanal (HTTPS over port 443) om en liste over handlinger, der skal gennemføres, på et bestemt tidspunkt hver dag
Apps til enhedsadministration	Xerox Device Agent Partner Edition til overvågning af netværksforbundne udskrivningsenheder	Intern	Hver enkelt app af typen Xerox Device Agent registrerer en webbaseret proxyserver (automatisk eller videresendt til en bestemt adresse)
		Intern	Hver enkelt app af typen Xerox Device henter udskrivningsenhedens funktioner på tværs af flåden via SNMP
		Intern	Each Xero® Device Agent app modtager udskrivningsenhedskonfiguration på tværs af flåden via SNMP
		Intern	Hver enkelt app af typen Xerox Device Agent modtager status om udskrivningsenheden på tværs af flåden via SNMP

Implementeringsmetode	Anvendt app	Datastrøm på netværket	Driftsevne pålagt et netværk
		Intern	Hver enkelt app af typen Xerox Device Agent modtager forbrugsdata for udskrivningsenheder på tværs af flåden via SNMP
		Intern	Hver enkelt app af typen Xerox Device Agent kan anmode om, at enheden udskriver en konfigurationsrapport
		Intern	Hver enkelt app af typen Xerox Device Agent kan åbne en udskrivningsenheds webside
		Intern	Hver enkelt app af typen Xerox Device Agent kan opgradere printerenhedens software via indsendelse af udskriftsjob. (. DLM-fil over port 9100)
		Ekstern (**kun udgående)**	Hver enkelt app af typen Xerox Device Agent krydser virksomhedens firewall for at få adgang til internettet (HTTPS over port 443)
		Ekstern (**kun udgående)**	Hver enkelt app godkendes med dens certifikat Remote Xerox Communication Server, før der transmitteres nogen dataegenskaber
		Ekstern **(kun udgående)**	Hver enkelt app af typen Xerox Device Agent transmitterer automatisk udskrivningsenhedens egenskabsdata igennem en krypteret kanal (HTTPS over port 443) til Xerox® Communication Servers på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Hver enkelt app af typen Xerox Device Agent forespørger automatisk Communication Servers om en liste over handlinger, der skal gennemføres, igennem en krypteret kanal (HTTPS over port 443) på et bestemt tidspunkt hver dag
Apps til enhedsadministration	Xerox® Device Manager til overvågning af netværksforbundne udskrivningsenheder	Intern	Apps af typen Xerox Device Manager/Xerox Device Agent registrerer en webproxyserver (automatisk eller videresendt til en bestemt adresse)
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent henter udskrivningsenhedsfunktioner på tværs af flåden via SNMP
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent henter udskrivningsenhedskonfiguration på tværs af flåden via SNMP
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent henter udskrivningsenhedsstatus på tværs af flåden via SNMP
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent modtager forbrugsdata for udskrivningsenheden på tværs af flåden via SNMP
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent kan anmode om, at enheden udskriver en konfigurationsrapport
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent kan åbne en udskrivningsenheds webside
		Intern	Apps af typen Xerox Device Manager/Xerox Device Agent kan opgradere printerenhedens software via indsendelse af udskriftsjob
		Intern	Apps af typen Xerox Device Manager understøtter SNMPv3-kommunikation med udskrivningsenheder

Implementeringsmetode	Anvendt app	Datastrøm på netværket	Driftsevne pålagt et netværk
		Intern	Appen Xerox Device Manager kan foretage ændringer af udskrivningsenhedens konfiguration via SNMP og webgrænseflade
		Intern	Appen Xerox Device Manager henter jobbaserede regnskabslogfiler fra visse Xerox® MFP'er
		Intern	Appen Xerox Device Manager administrerer/håndhæver udskrivningskontrolpolitikker
		Ekstern **(kun udgående)**	Apps af typen Xerox Device Manager/Xerox Device Agent krydser virksomhedens firewall for at opnå adgang til internettet (HTTPS over port 443)
		Ekstern (**kun udgående)**	Hver enkelt app godkendes med dens certifikat Remote Xerox Communication Server, før der transmitteres nogen dataegenskaber
		Ekstern **(kun udgående)**	Apps af typen Xerox Device Manager/Xerox Device Agent transmitterer automatisk udskrivningsenhedsdata til Xerox® Communication Servers igennem en krypteret kanal (HTTPS over port 443) på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Apps af typen Xerox Device Manager/Xerox Device Agent forespørger automatisk Xerox Communication Servers om en liste over handlinger, der skal gennemføres (HTTPS over port 443), på et bestemt tidspunkt hver dag
	Apps af typen Device Manager	Ekstern, dobbeltrettet	Xerox Device Manager kontakter Xerox Services Manager dagligt og giver administratorer mulighed for at ændre indstillinger på afstand og undgå behovet for serviceopkald på stedet.

9. Sikkerhedsfunktioner

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) TIL XEROX®

Simple Network Management Protocol (SNMP) er det mest udbredte netværksstyringsværktøj til kommunikation mellem netværksstyringssystemer og netværksprintere. Apps af typen Device Management anvender SNMP under registreringsoperationer for at indhente detaljerede oplysninger om udskriftsenheden. Apps af typen Xerox® Device Management understøtter protokollerne SNMP v1/v2 og v3. Se de pågældende certificeringsvejledninger til appen Xerox® Device Management for at få specifikke detaljer.

SNMP v3-rammen understøtter flere sikkerhedsmodeller, som kan eksistere samtidigt i en SNMP-entitet. SNMPv3 omfatter strammere sikkerhed ved at føje kryptografisk sikkerhed til SNMPv2. Yderligere er SNMPv3 bagudkompatibel med tidligere versioner og anvendes i vidt omfang på tværs af robuste netværk.

Apps af typen Xerox Device Management (Centre Ware® Web/Xerox Device Manager, Xerox Device Agent) kan kommunikere med enhedsplatforme, der er i overensstemmelse med Federal Information Processing Standard FIPS 140-2 i deres implementeringer af SNMPv3.

Apps af typen Xerox Device Management anvender ikke tjenesten Windows SNMP eller tjenesten Windows SNMP Trap. Hvis disse enheder tidligere er blevet installeret, **skal** de deaktiveres på enhver personlig computer (pc) eller server, hvor appen Xerox Device Management er installeret.

Apps af typen Xerox Device Management anvender en Xerox-udviklet SNMP-agent, der:

- Indeholder en særlig indkodnings-/afkodningsmekanisme
- Er komplet .NET-administreret
- Anvender .NET runtime eksekverbar – dette leverer øget sikkerhed med henblik på at forhindre angreb på softwaresårbarheder såsom ugyldige pointermanipulationer, bufferoverskridelser og bundet kontrol.

Apps af typen Xerox Device Management anvenderbruger de sikkerhedsfunktioner, der er tilgængelige fra Windows-operativsystemet (OS), herunder:

- Brugergodkendelse og -autorisation
- Konfiguration og administration af tjenester
- Implementering og styring af gruppepolitik

Windows Internet Connection Firewall (ICF), herunder:

- Indstillinger for sikkerhedslogning
- ICMP-indstillinger

Apps af typen Xerox Device Management: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE-appen Microsoft® SQL Server samt **Xerox Device Manager** anvender Microsoft® SQL Server.

Apps af typen Xerox Device Management kan konfigureres til at udnytte de øvrige Microsoft®-sikkerhedsfunktioner, som kan omfatte (hvor det er relevant):

- Aktivering af brugerkontoregistrering
- Kryptering af Domain Name System (DNS)
- Begræns brugerkontorettigheder for at opnå adgang til databasen (dvs. indehaverrettigheder til databaser)
- Implementering af brugerdefinerede portnumre

En Xerox-registreringsnøgle og en gyldig Xerox-konto er påkrævet for at overføre data til de eksterne Xerox-kommunikationsservere.

Kommunikation med apps af typen Xerox Device Management kan blive påvirket af Windows Internet Connection Firewall. (Vi **anbefaler**, at kunder hvidlister Xerox URL på kundens firewall (*.support.xerox.com) og antgiver den IP-adresse, der kan åbne URL'en**.**)

Apps af typen Xerox Device Management kører som en baggrundsproces ved hjælp af lokale systemkontolegitimationsoplysninger med henblik på at oprette automatiske forespørgsler af netværksprintenheder via SNMP og med jævne mellemrum sende udskrivningsenhedsegenskaber tilbage til Xerox's kommunikationsservere

Adgang til grænseflader og funktioner tilhørende apps af typen Xerox Device Manager kontrolleres igennem følgende rollebaserede rettigheder:

- Centre Ware® Web Administrators, Centre Ware® Web Power-brugere, Centre Ware® Web SQL-brugere, Centre Ware®-webadministratorer og Centre Ware®-webkundegrupper.
- Brugernavne og adgangskoder til apps passerer ikke netværket. Adgangstokens bruges i stedet (af Windows® OS-design).
- Appen Xerox Device Manager leverer kontrolbaseret sikkerhed for udskriftsindsendelse ved at begrænse job på baggrund af farveforbrugspolitik, dokumenttype, jobomkostninger, tidspunkt på dagen, brugergruppeadgangskontrol, duplekspolitik, tilladte jobvisninger og udskriftskvoter.

Bemærk: Brug af SNMP af enhver app af typen Xerox® Remote Services udgør ikke en sikkerhedsrisiko for en kundes it-miljø, eftersom al SNMP-baseret trafik, der genereres eller forbruges af disse applikationer, foregår på kundens intranet bag firewallen. Windows SNMP-tjenesten og Windows SNMP Trap-tjenesten er som standard ikke aktiveret i Windows OS.

Virksomhedsbaseret sikkerhedstilstand

Den ***planlagte*** synkroniserng af appen Xerox Device Agent til den sikre kommunikationsserver er som standard indstillet til *dagligt*. Bemærk, at tidspunktet på dagen kan vælges frit.

Der findes to virksomhedsbaserede sikkerhedstilstande: **Normal** og **Låst ned.**

I tilstanden **Normal** kontakter appen Device Management Xerox Services Manager dagligt. Indstillinger kan ændres uden behov for besøg på stedet, selv når afstemningsplaner er slået fra. ***(Anbefalet tilstand***).

I **nedlukningstilstand** er der udover printerrelateret datasynkronisering ingen kommunikation med Xerox Services Manager, og indstillingerne skal ændres på stedet. Yderligere rapporteres Xerox Device Agent-maskinens og printeres IP-adresser ikke til kommunikationsserveren. Denne tilstand begrænser alle andre fordele ved fjerntjenester til at omfatte automatisk fakturering og forsyninger samt diagnostiske data, der anvendes til teknisk support.

Bemærk: Hvis en Xerox Device Agent-version ikke indeholder fanen Corporation Security Mode, fungerer den i normal tilstand.

10. Netværkspåvirkning

Virksomhedens netværksretningslinjer vil typisk aktivere eller deaktivere specifikke netværksporte på routere og/eller servere. De fleste it-afdelinger bekymrer sig over de porte, som applikationen anvender til udgående trafik. Deaktivering af specifikke porte kan påvirke appens funktionalitet. Se tabellen nedenfor for at få oplysninger om specifikke porte, der anvendes af applikationens processer. Hvis appen skal scanne på tværs af flere netværkssegmenter eller undernet, skal routere tillade de protokoller, der er tilknyttet disse portnumre.

Protokoller, porte og øvrige relaterede teknologier

Tabel 7 omfatter oplysninger om de protokoller, porte og teknologier, der anvendes i Xerox® Remote Services:

Portnummer	Protokol	Beskrivelse af brug	Datastrøm på netværket
Afhænger af protokoller i øvre lag	**Internet Protocol (IP)**	**Underlæggende transport af al datakommunikation**	**Intern + ekstern (kun udgående)**
Ikke relevant	Internet Control Message Protocol (ICMP)	Registrering af udskrivningsenheder + fejlfinding	Intern
25	Simple Mail Transport Protocol (SMTP)	Udskrivningsenhed + e-mail-alarmer om apps af typen fjern-proxy	Intern
53	Domain Name Services (DNS)	Anvendes til DNS-baserede søgefunktioner til udskrivningsenheder	Intern
80	Hyper Text Transport Protocol (HTTP)	Udskrivningsenhed websideforespørgsler + appen Device Management websideforespørgsler	Intern
135	Remote Procedure Call (RPC)	Registrering af udskrivningsenheder	Intern
161	Simple Network Management Protocol (SNMP v1/v2C/v3)	Branchens standardprotokol, der benyttes til at registrerede netværksudskrivningsenheder + Hent status, tællere og forsyningsdata + Hent og anvend konfiguration af udskrivningsenhed. Navne på standardfællesskaber = "offentlig" (GET), "privat" (SET)	Intern

Portnummer	Protokol	Beskrivelse af brug	Datastrøm på netværket
443	Hyper Text Transport Protocol Secure (HTTPS)	Udskrivningsenhed sikre websideforespørgsler (hvis løsningen er konfigureret) + fjernproxt app sikker websideforespørgsel (hvis løsningen er konfigureret) + Udskrivningsenhed dataoverførsel tilbage til Xerox®'s kommunikationsservere + udskrivningskontrolkommunikation tilbage til Xerox® Device Manager	Intern + ekstern (kun udgående)
515, 9100, 2000, 2105	TCP/IP LPR og indsendelse af Raw Port-udskrivningsjob	Udskrivningsenhed softwareopgradering + Udskriv testside diagnosticering	Intern

11. Best practices inden for sikkerhed

- Hold altid udskrivningsenheder opdateret med den nyeste firmware/software. Xerox overvåger sårbarheder nøje og sender proaktivt kunderne sikkerhedsrettelser og opdateringer, når det er nødvendigt.
- Deaktiver ubrugte porte og protokoller på udskrivningsenheder, mår det er muligt. Dette gøres typisk ved webbrugergrænsefladen (UI) for printenheder i kontorklasse og lokal brugergrænseflade (UI) på printenheder i produktionsklasse.
- Udnyt relaterede funktioner til brugeradgangskontrol på udskrivningsenheder, hvis de er tilgængelige. Dette gøres typisk ved webbrugergrænsefladen (UI) for printenheder i kontorklasse og lokal brugergrænseflade (UI) på printenheder i produktionsklasse.
- Benyt sikre protokoller, når det er muligt. Dette gøres typisk ved webbrugergrænsefladen (UI) for kontorbaserede printenheder og lokal brugergrænseflade (UI) på printenheder i produktionsklasse.
- Aktiver sikkerhedsfunktioner, der er indlejret i enheden (f.eks. billedoverskrivning, scanningsdatakryptering, printstreamkryptering, diskkryptering, sikker udskrivning, krypteret .pdf, CAC/PIV-adgangsgodkendelse).

Der findes yderligere oplysninger om Remote Services @ Xerox på Xerox.com/RemoteServices.

Der findes yderligere og specifikke oplysninger om sikkerhedsmekanismerne og -funktionerne inden for apps af typen Xerox Device Management i de pågældende vejledninger:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Uanset om der er tale om enheds- eller indholdssikkerhed, er Xerox på forkant med proaktiv sikkerhed i forhold til nutidens nye trusler. Besøg www.xerox.com/security for at få adgang til et komplet udvalg af sikkerhedsoplysninger, opdateringer, bulletiner, hvidbøger, patches og meget mere.