Xerox® Remote Services

Informasjonsbrosjyre om sikkerhet

Versjon 2.0
Remote Services globalt
Xerox® Technology Information Management

Januar 2017

BR19369

Av og til gjøres det endringer i dette dokumentet. Endringer, tekniske unøyaktigheter og skrivefeil vil bli korrigert i senere utgaver.

IS 614672/IS 514590

Dokumentversjon: 2.0 (januar 2017).

Innhold

Generelt formål og målgruppe

Dette dokumentet er ment å tjene som en veiledning til å rulle ut Xerox® Remote Services for skrivere fra Xerox og andre merker, som står i et nettverksmiljø hos kunden. Det inneholder detaljert informasjon om de omfattende sikkerhetstiltakene Xerox® Remote Services inkluderer.

Dette dokumentet er ment for tekniske forhandlere, nettverksansvarlige og IT-sikkerhetsfolk som er interessert i funksjonene i Remote Services og de sikkerhetsmessige aspektene ved implementeringen av dem.

Vi anbefaler at dokumentet gjennomgås i sin helhet for å sikre at produktene og tjenestene til Xerox® blir riktig anvendt i kundens nettverk.

Remote Services

Informasjon er svært verdifullt for virksomheten, og sikkerhet er av overordnet betydning for alle virksomhetens aktiva, inkludert multifunksjonsskrivere (MFPer) som står i nettverk. Med den utbredelsen «alt-i-ett»-konseptet har i dag, er det lett å undervurdere de utfordringene det gir å administrere en hel flåte av multifunksjonsskrivere og samtidig opprettholde et akseptabelt sikkerhetsnivå. Xerox® vet hvor komplekst dette er og er svært oppmerksomme på kundenes sikkerhetsbehov. Xerox® Products, Xerox® Systems og Xerox® Remote Services er utformet for integrasjon med våre kunders nåværende arbeidsflyt ved hjelp av den nyeste sikkerhetsteknologien.

Informasjonsbrosjyren om den innebygde sikkerheten i Xerox® Remote Services er ment for å hjelpe kunden med å forstå og ta i bruk den riktige Remote Services-løsningen som er kompatibel med nettverkets infrastruktur. Kundens nåværende nettverksarkitektur vil avgjøre om det bør foretas endringer i internett-brannmuren, web-proxyservere eller annen sikkerhetsrelatert infrastruktur. Hvilken løsning, enhet og kontroller for Xerox® Remote Services som velges, avhenger av kundens policyer for informasjonssikkerhet (IS), og dette vil også bestemme hvilken driftsmetode som skal brukes.

Xerox ® Remote Services er tilgjengelig med visse utstyrsmodeller. Funksjonene gjør at skrivere kan driftes og vedlikeholdes fra en annen lokasjon ved å bruke attributtdata for skriveren som inkluderer*: skriveridentitet, skriveregenskaper, status, forbruk og detaljerte diagnostikkopplysninger*. Attributtdataene for skriveren overføres fra kundens nettverksmiljø, direkte fra skriveren (Device Direct), gjennom en driftet applikasjon (Device Management Application), eller via en kombinasjon av begge metodene ved hjelp av en sikret Xerox® Remote Services-kommunikasjonslinje. Både Xerox®-enheter og Xerox® Device Management-applikasjoner har et sertifikat som brukes til autentisering mot Xerox®-kommunikasjonsservere før overføringen av utskriftsattributtene kan skje. Transaksjoner med Xerox® Remote Services initieres alltid fra innsiden av kundens miljø og sendes utelukkende etter at de er autorisert av kunden.

Det USA-baserte Xerox® Communications Servers overholder de strenge kravene som stilles til administrasjon av informasjonssikkerhet. Xerox® Datacenters og Xerox® Remote Services-applikasjonen overholder de årlige kravene til SSAE (Statement on Standards for Attestation) No-16 og SOX (Sarbanes-Oxley Act) og er ISO 27001:2013-sertifisert.

Ingen kunde-bilder fra utskrift, faks, skanning, kopiering eller sensitiv informasjon blir overført til Xerox®-kommunikasjonsservere.

Kundens styringssystemer

Xerox® Device Management-applikasjoner har mulighet for å vise eksporterte attributtdatalogger fra enheten til gjennomsyn og verifisering før kryptering og overføring til eksterne Xerox®-kommunikasjonsservere. I veiledningen til Xerox® Device Management-applikasjonen finner du mer informasjon.

Noen små og mellomstore skrivere har en funksjon som gjør at kundene kan laste ned og vise skriverens attributtdata før kryptering og overføring til de eksterne Xerox®-kommunikasjonsserverne gjennom aktiveringen av Device Direct. For å se om en skriver har denne funksjonen, gå til skriverens Centreware Internet Services-side; fanen Status, lenken Smart eSolutions (eller Remote Services) og se under fanen Maintenance Assistant.

Xerox® Remote Services kan skreddersys etter kundens IS-policyer slik at de sterkt begrenser eller holder tilbake visse former for skriverattributter som kan overføres utenfor nettverket (f.eks. attributter relatert til nettverksadresser). Xerox® Device Management applikasjonsverktøy kan deaktivere utvalgte feler slik at de ikke overføres.

Kunden har også mulighet for å iverksette en *unntaksanmodning* ved inngåelsen av kontrakten for å **velge bort** Remote Services. Dette valget vil hindre all Remote Services-kommunikasjon og ekstern brukerstøtte for skriverne som tilhører den kontoen.

For å eskalere ekstern brukerstøtte kan kunden etter behov aktivere Remote Access-funksjonen for å motta ny programvare og sikkerhetsoppdateringer, og også for å reparere eller modifisere skriverkonfigurasjonen for å korrigere feil som blir diagnostisert. Remote Access tillater ikke at Xerox® ser på eller laster ned kundens dokumenter, data eller noen annen informasjon som befinner seg i eller sendes gjennom skriveren eller kundens informasjonssystemer. Unntaket er når en kunde er i kontakt med noen fra brukerstøtten hos Xerox om et vanskelig problem, og det viser seg at det er nødvendig med mer informasjon for å feilsøke problemet. I så fall kan en kunde avgjøre at Xerox får tilgang til lokalt lagrede logger på maskinen, som inkluderer sensitive opplysninger.

Vi anbefaler at IT-medarbeidere og sikkerhetsansvarlige leser dette dokumentet i sin helhet for å få en full forståelse av de forskjellige funksjonene, kravene og virkemåtene til Xerox® Remote Services og hvordan de sikrer etterlevelsen av vår kunders IT-sikkerhetspolicyer.

Ytterligere informasjon om databeskyttelse for Xerox®-produkter, industripartnerskap og sertifisering finner du på http://www.xerox.com/security.

Utrulling

Kunden kan velge mellom to like sikre utrullingsmodeller for Xerox® Remote Services:

- **Device Direct-modell** – Device Direct gjør at enheter kan kommunisere direkte med de eksterne Xerox®-kommunikasjonsserverne via Internett gjennom kundens brannmur.

- **Device Management-applikasjonsmodell** – En Xerox® Device Management-applikasjon (også kalt Device Manager) kan tas i bruk i en kundes nettverk for å samle inn visse dataattributter fra skriverne. Flere skriverattributter blir samlet inn og deretter overført på en sikker måte til de eksterne Xerox®-kommunikasjonsserverne.

- **Kombinasjonsmodell** – implementering av både Device Direct- og Device Management-applikasjonsmodeller.

Alle utrullingsmodeller for Xerox ® Remove Services utnytter standard webbaserte protokoller og porter for å opprette en sikker, kryptert kanal for overføring av skriverattributter eksternt til Xerox®-kommunikasjonsservere som er lokalisert i Xerox®-datasentre med redundant sikring.

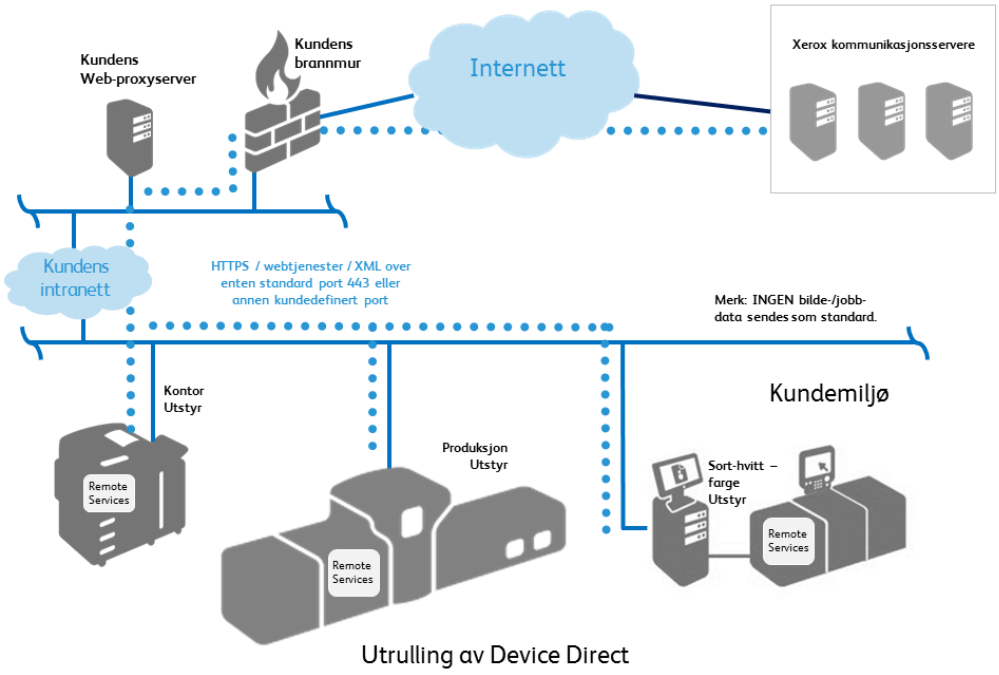
Hvilken utrullingsmodell som velges, avhenger av våre kunders IS-policyer og regler for behandling av overføringen av skriverattributtene og hva slags utskriftsløsning og hvilke skrivere som er kjøpt fra Xerox® (enkle eller styrte utskriftstjenester).

Utrulling av Device Direct

Remote Services-modulen som er integrert i Xerox®-enhetene, benytter en sikker TLS 1.2-forbindelse (Transport Layer Security) over port 443 for å kommunisere med de eksterne Xerox®-kommunikasjonserverne.

- Skrivere som står i kundens miljø, initierer direkte all kommunikasjon med de eksterne Xerox®-kommunikasjonsserverne. Det krever standard brannmurkonfigurasjon ute hos kunden for å muliggjøre denne kommunikasjonen.
- Det må brukes en gyldig URL for de eksterne Xerox®-kommunikasjonsserverne.
- Xerox®-kommunikasjonserverne befinner seg innenfor en sikker brannmur og er ikke tilgjengelige fra Internett.

Figur 1



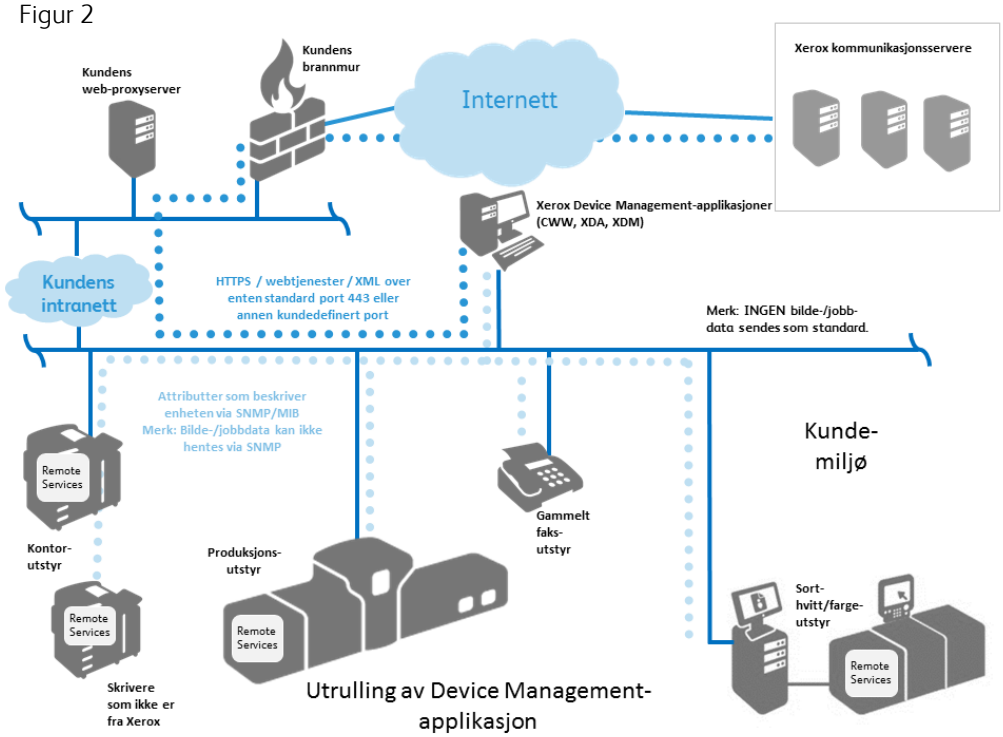
Utrulling av Device Direct

Utrulling av Device Management-applikasjon

Device Management-applikasjonene (dvs. **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition og Xerox® Device Manager)** benytter også en sikker, kryptert forbindelse med TLS (Transport Layer Security) 1.2 over port 443 for å kommunisere med de eksterne Xerox®-kommunikasjonsserverne. Det benyttes også andre funksjoner for å øke sikkerheten til denne kanalen, som opprettes ved installasjonen av Device Management-applikasjoner og inkluderer følgende:

- Device Management-applikasjonen inne i kundens miljø initierer all kommunikasjon med de eksterne Xerox®-kommunikasjonsserverne. Det kreves standard brannmurkonfigurasjon ute hos kunden for å muliggjøre denne kommunikasjonen.
- Det må brukes en gyldig URL for de eksterne Xerox®-kommunikasjonsserverne.
- Xerox®-kommunikasjonserverne befinner seg innenfor en sikker brannmur og er ikke tilgjengelige fra Internett.
- Det må enten brukes en gyldig konto-ID eller stedsidentifisering og en registreringsnøkkel for Xerox®-kommunikasjonsserver for å få tilgang til en av tjenestene på Xerox®-kommunikasjonsserverne.
- Device Management-applikasjonen anmoder om en registrering med den eksterne Xerox®-kommunikasjonserverne ved hjelp av fullmaktene til et korrekt autentiseringssertifikatet.
- De eksterne Xerox®-kommunikasjonsserverne godkjenner fullmaktene og aksepterer anmodningene.
- Device Management-applikasjonen autentiserer de eksterne Xerox®-kommunikasjonsserverne og aktiverer tjenesten.

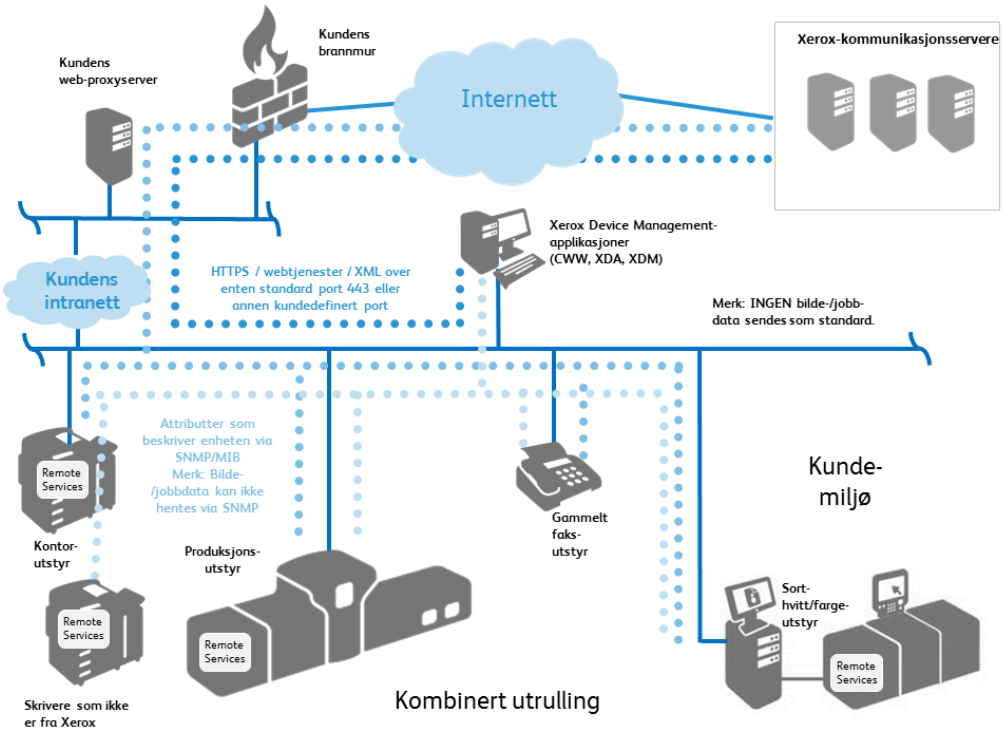
Figur 2



Kombinert utrulling

Kombinasjonsutrullingen benyttes når en kunde kjøper flere forskjellige Xerox-vedlikeholdsavtaler for skriverne sine. Når en Xerox®-skriver blir installert i et nettverk for første gang, er den automatiske responsen til Xerox® Remote Services å forsøke å opprette en direkte forbindelse til Xerox®-kommunikasjonsserverne.

Figur 3



Dataoverføring og utnyttingsgrad

Datakilder

Skriverens dataattributter blir samlet inn til Xerox® Remote Services fra følgende kilder:

- Xerox® kontornettverksskrivere
- Nettverksskrivere som ikke er fra Xerox®
- Xerox® produksjonsskrivere
- Xerox® Device Management-applikasjoner

Xerox® kontorenheter

Xerox®-skrivere for kontorbruk overfører data fra skriverenheten i XML-format (eXtensible Markup Language) med en komprimert fil (.zip). Hver fil blir så overført via en kryptert kanal til de eksterne Xerox®-kommunikasjonsserverne.

Tabell 1 identifiserer skriverdataattributtene som kan overføres, samt beskrivelsen av dem.

Dataattributter	Beskrivelse
Skriverens identitet	Inkluderer modell, fastvarenivå, modulens serienumre og installasjonsdato.
Skriverens nettverksadresse	Inkluderer MAC-adresse (Media Access Control) og subnet-adresse.
Skriveregenskaper	Inkluderer detaljert maskinvarekonfigurasjon, detaljert programvarekonfigurasjon, funksjoner/tjenester som støttes, strømsparemodus osv.
Skriverstatus	Inkluderer generell status, detaljerte varsler, historikk med siste 40 feil, informasjon om fastkjørt papir osv.
Skrivertelleverk	Inkluderer telleverk for fakturering, utskrifter, kopiering, faks, store utskrifter, skann-til-destinasjon, brukerstatistikk osv.
Forbruksartikler for skriver	Inkluderer forbruksartikkelens navn, type (f.eks. bilde, etterbehandling, papirmedia), nivå, kapasitet, status, størrelse osv.
Detaljer om maskinutnyttelse for utskriftsjobber	Inkluderer detaljerte utskriftsrelaterte tellere, strømstatus, detaljerte kvanta for enheter kunden kan skifte ut (CRU), detaljerte data om CRU-feil og -distribusjon, bruk av integrert OCR (Optical Character Recognition), distribusjon av utskriftsjobblengde, distribusjon av bruk av papirmagasin, installert papir, distribusjon av papirtyper, distribusjon av papirstørrelser, distribusjon av dokumentlengde, settnummer, HFSI-data, NVM-data, distribusjon, telling av markert piksel, gjennomsnittlig dekning for hver farge, feil/fastkjøring, detaljerte skann-relaterte tellere.

Dataattributter	Beskrivelse
Teknisk / feilsøking	Inkluderer detaljert feilsøkingsinformasjon som kanskje ikke er med i det ovenstående datasettet. Dataene kan inkludere PIIer som brukernavn, e-postadresser og jobbdata. Disse dataene blir sendt med eksplisitt tillatelse fra kunden og er kun ment til eskalert brukerstøtte.

Merk: Filen og innholdet i dataene varierer etter produktmodell.

Xerox® produksjonsenheter

Xerox®-produksjonsenheter overfører enhetens attributtdata i XML-format (eXtensible Markup Language) med en komprimert fil (.zip). Hver fil blir så overført vi en kryptert kanal til de eksterne Xerox®-kommunikasjonsserverne.

Tabell 2 identifiserer enhetens dataattributter og beskrivelsen av dem, som kan overføres.

Dataattributter	Detaljert beskrivelse av dataattributter
Skriverens identitet	Inkluderer modell, modulens fastvarenivå, modulens serienumre, modulens installasjonsdatoer, kundens kontaktopplysninger, lisensinformasjon og stedsadresse, hvis tilgjengelig.
Skriverens nettverksadresse	Inkluderer MAC-adresse (Media Access Control) og subnet-adresse.
Skriveregenskaper	Inkluderer detaljert maskinvarekonfigurasjon, detaljert programvarekonfigurasjon, funksjoner/tjenester som støttes osv.
Skriverstatus	Inkluderer aktive statuser, feilhistorikk, DFE-hendelseslogg, dataoverføringshistorikk
Skrivertelleverk	Inkluderer målere for fakturering, telleverk for utskrifter, kopiering, store utskrifter, produksjon, skann-til-destinasjon for rimelige produksjonsmodeller osv.
Forbruksartikler for skriver	Inkluderer produsent, modell, serienummer, navn, type, nivå, kapasitet, status, levetidstelleverk osv.
Detaljer om maskinutnyttelse for utskriftsjobber	Inkluderer HFSI-data, NVM-data, utskifting av deler, DFE-logger, detaljerte diagnostiske data, feiloppretting.
Teknisk / feilsøking	Inkluderer ustrukturerte, detaljerte data relatert til feilsøking. Er kun ment for tredjelinjes brukerstøtte.
Kundejobb-relatert	Med en Xerox® produksjonsskriver er det mulig å reprodusere jobbrelaterte data som kan benyttes til eskalert brukerstøtte via kryptert PostSXcript til Xerox. Kunden kan bestemme om denne funksjonen skal aktiveres. Hvis kunden bestemmer seg for å overføre jobbrelaterte data (dvs. kryptert PostScript) tilbake til Xerox, behandles dataene iht. Xerox' IS-policyer og -standarder.

Det finnes et scenario med eskalert brukerstøtte hvor det benyttes detaljert feilsøkingsinformasjon med dataattributter som ikke er inkludert i datasettet i tabell 1–3. Disse dataene blir sendt med eksplisitt tillatelse fra kunden og behandles iht. Xerox-sikre IS-policyer og -standarder.

Merk: Filen og innholdet i dataene varierer avhengig av produktmodell.

Xerox Device Management-applikasjoner

Xerox® Device Management-applikasjoner (dvs. Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**) og Xerox® Device Manager (**XDM**) overfører skriverattributtdataene i XML-format (eXtensible Markup Language) ved hjelp av en komprimert fil (.zip). Filen blir deretter kryptert og overført via krypterte kanaler til de eksterne Xerox®-kommunikasjonsserverne.

Tabell 3 viser enhetens dataattributter og beskrivelsen av dem, som kan sendes via Xerox® Device Management-applikasjonen.

Dataattributter	Detaljert beskrivelse av dataattributter
Skriverens identitet	Inkluderer produsent, modell, beskrivelse, fastvarenivå, serienummer, gjenstandsmerker, systemnavn, kontaktperson, stedsadresse, administrasjonsmaskin (desktop), faksnummer og kønavn.
Skriverens nettverksadresse	Inkluderer MAC-adresse, IP-adresse, DNS-navn, subnettmaske, IP default gateway, siste kjente IP-adresse, endret IP-adresse, tidssone, IPX-adresse, IPX eksternt nettverksnummer, IPX-skriverserver.
Skriveregenskaper	Inkluderer installerte komponenter, komponentbeskrivelser, funksjoner/tjenester som støttes, skriverhastighet, fargestøtte, etterbehandlingsfunksjoner, støtte for tosidig utskrift, markedsføringsteknologi, harddisk, RAM, språkstøtte, brukerdefinerte funksjoner.
Skriverstatus	Inkluderer generell status, detaljerte varslinger, lokale konsollmeldinger, komponentstatus, data relatert til statusinnhenting, søkedato, søkemetode/-type, enhetens oppetid, støtte/aktivering av traps.
Skrivertelleverk	Inkluderer telleverk for fakturering, utskrifter, kopiering, faks, store utskrifter, skanning, samt brukerstatistikk og målsetning for volum.
Forbruksartikler for skriver	Inkluderer forbruksartikkelens navn, type (f.eks. bilde, etterbehandling, papirmedia), nivå, kapasitet, status, størrelse osv.
Detaljer om bruk av skriveren	Brukerbaserte jobbsporingsdata som inkluderer jobbkarakteristikker (ID, dokumentnavn, dokumenttype, jobbtype, farge, tosidig, papirtype, format, sider, sett, feil), mål (skriver, modell, DNS-navn, IP-adresse, MAC-adresse, serienummer), resultatet av å skrive ut jobben (overføringstidspunkt, jobbutskriftstid, sider skrevet ut, sider skrevet ut i farge/sort-hvitt, fargemodus benyttet, N-up), regnskapsdata (chargeback-kode, chargeback-pris, regnskapskilde), utskriftsjobbens kilde (arbeidsstasjon, skriverservernavn/MAC-adresse, navn på kø, port, brukernavn, bruker-ID), Xerox management-data (sendt til Xerox® Services Manager).
Device Management-identitet	Inkluderer informasjon om applikasjonsvert-PCen, som DNS-navn, IP-adresse, operativsystem, operativsystemtype, hovedprosessor, RAM (tilgjengelig versus i bruk), harddisk (tilgjengelig versus i bruk), områdenavn, app-versjon, utløpsdato for app-lisensen, .NET-versjon, discovery component-versjon, størrelse på hoveddatabasen, antall skrivere som kan nås / ikke nås, kritiske tjenester som kjører.

Dataattributter	Detaljert beskrivelse av dataattributter
Device Manager Corporation Security Mode	**Vanlig modus** = Xerox® Device Agent kontakter Xerox® Services Manager daglig. Innstillingene endres eksternt uten å måtte besøke lokasjonen, selv når planlagt henting er slått av. **Låst modus** = Bortsett fra skriverrelatert datasynkronisering er det ingen kommunikasjon med Xerox® Services Manager, og innstillingene må endres på stedet. Xerox® Device Agent-maskinen og skriverens IP-adresser blir rapportert til Xerox® Services Manager.
Device Management-utskriftskontroll	Inkluderer navnet til sluttbruker-PCen, skriverserver, utskriftskø, tidsstempel på avvik, dokumentnavn, sluttbrukers brukernavn, tosidig jobb, fargejobb, jobbens totale antall utskrifter, jobbens pris, tiltak, varsling til sluttbruker, melding vist, navn på utskriftspolicy, hvilken regel iht. utskriftspolicy som er anvendt.

Ekstern administrasjon av skrivere

Xerox®' kundestøtte kan gjøre følgende via Xerox® Device Management-applikasjonen. Disse tiltakene forutsetter at kunden har tillatt det, og gjøres for å løse de problemene som er beskrevet i **Tabell 4** nedenfor.

Data-	beskrivelse
Tiltak på selve skriveren	• **Hent skriverstatus** = hente den seneste statusen fra skriveren • **Ta en omstart på enheten** = slå skriveren av og på • **Oppgrader enheten** = installer ny programvare/fastvare på skriveren (.DLM over port 9100) • **Feilsøk enheten** = ping skriveren + hent siste status fra den • **Skriv ut testside** = send en testjobb til en skriver for å validere utskriftsbanen (genererer en konfigurasjonsrapport) • **Start administrasjon av enhet** = initier periodiske skriverdataoverføringer til de eksterne Xerox®-kommunikasjonsserverne **Merk:** Hver av disse handlingene kan deaktiveres når ønskelig, i seksjonen for administrasjonskonfigurasjon i Xerox® Device Management-applikasjoner som støtter denne funksjonen.
Tiltak på selve skriveren	• **Ta en omstart på enheten** = slå skriveren av og på • **Skriv ut testside** = send en testjobb til en skriver for å validere utskriftsbanen (genererer en konfigurasjonsrapport)
Handlinger som utføres i Device Management-applikasjonene	Innstillinger som kan endres i hver device management-applikasjon inkluderer søkfunksjon, hyppighet av dataeksport, SNMP-kommunikasjon (gjenforsøk, tidsavbrudd, gruppenavn, alarmprofiler og oppdateringsfrekvens for programvaren som foretar automatisk enhetsbehandling).

Systemkrav for Device Management-applikasjoner

Minstekravene varierer noe alt etter hva som tilbys. Se i brukerveiledningen, sikkerhetsevalueringsveiledningen og/eller sertifiseringsveiledningen om hvilke grunnleggende krav som gjelder for hver enkelt device management-applikasjon. Ytterligere detaljer finnes her: http://www.support.xerox.com/support/enus.html

I installasjonen følger det med en .readme-fil, som lister opp ytterligere og spesifikke systemkrav for hver enkelt device management-applikasjon som blir installert.

- Vi anbefaler at vertsmaskiner har et støttet operativsystem fra Microsoft® Corporation. Xerox® Device Management-applikasjoner kan imidlertid kjøres i et Macintosh OS-miljø, hvis det benyttes en Parallels Desktop-emuleringsprogramvare. (I sin nåværende versjon kan du ikke kjøre Xerox® Device Management-applikasjonen i et Macintosh-miljø.) I veiledningene til Xerox® Device Management-applikasjonene finner du mer informasjon.

- Vi anbefaler at vertsmaskiner holdes oppdatert med de siste viktige patchene og servicepakkene fra Microsoft® Corporation.

- Nettverks-TCIP/IP (Transmission Control Protocol/Internet Protocol) må være lastet og i bruk.

- Internettforbindelse er nødvendig

- Man må være administrator på klientmaskinen for å kunne installere Device Management-applikasjonsprogramvare på den.

- Krever SNMP-aktiverte enheter og mulighet for å rute SNMP over nettverket. Det er ikke nødvendig å aktivere SNMP på datamaskinen som Xerox® Device Management-applikasjoner blir installert på, og heller ikke på noen andre nettverksmaskiner.

- Du må installere Microsoft®.NET Framework 4.6 (fullversjon) før du installerer applikasjonen.

- Applikasjonen bør ikke installeres på en PC hvor andre SNMP-baserte applikasjoner eller andre Xerox® Device Management-verktøy er installert, ettersom de kan innvirke på hverandre.

Konfigurasjoner som ikke støttes

- Installasjon på en datamaskin som har en annen Xerox® Device Management-applikasjon, slik som Xerox® Device Manager.

- Ethvert Unix®- eller Linux®-operativsystem

- Microsoft®-operativsystemer som er utgått, slik som Windows NT® 4.0, Windows® Media Center, Windows® XP og Windows® Server 2000 og 2003.

- Andre virtuelle miljøer enn VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Denne applikasjonen kan fungere i andre virtuelle miljøer, men er ikke blitt testet med slike.

Xerox® Business Process og Services

Dataene som mottas av Xerox®-kommunikasjonsserverne fra kontor- og produksjonsbaserte skrivere fra Xerox® og Xerox® Device Management-applikasjoner, blir benyttet av de følgende Xerox-forretningsprosessene:

Forretningsprosessnavn	Beskrivelse
Automatisk avlesing av måler	Det blir automatisk generert en regning fra målerdataene som mottas fra skrivere.
Automatisk etterfylling av forbruksmateriell / automatisk etterfylling av deler	Toner blir automatisk sendt til kunden når et varsel om at det er lite forbruksmateriell igjen blir mottatt fra skrivere. Utskiftbare komponenter på skriveren blir automatisk sendt til kunden når det er behov for det. Dette er alternativer som bare er tilgjengelige for kunder som har valgt kontrakter med måleravlesing.
Tilgjengelighet (vedlikeholdsassistent)	Detaljert informasjon om feil kan hentes opp av servicepersonell fra Xerox når nødvendig, for å forberede et besøk på stedet eller fjerndiagnostisere og løse problemer.
Støtte på nivå 3 (teknisk/feilsøking)	Personell som gir produktstøtte, kan feilsøke vanskelige problemer når de blir gitt tilgang til detaljerte tekniske logger og feilsøkingslogger.

Grunnleggende skriverdata blir komprimert, overført, beholdt og arkivert i et ISO-27001-sertifisert Xerox® datasenter, og tas vare på iht. Xerox® oppbevaringspolicyer for bedriftsdata.

Arbeidsprosessene og praksisene som støtter og beskytter Xerox® Backoffice Remote Services-programvaresystemer, bygger på beste praksis iht. ITIL samt Xerox informasjonssikkerhetspolicyer som er basert på ISO 27001-standarder. Kundene kan være sikre på at styringen av dataintegritet, personvern og beskyttelse er iht. beste praksis.

Opplysninger om teknologi

Denne seksjonen inneholder ytterligere tekniske detaljer som typisk kreves av IT-team og sikkerhetsansvarlige i tilknytning til risikostyring, gjennom å sørge for sikre utviklingsmetoder – og dermed at skrivere og Device Management-applikasjoner kan bli sertifisert for bruk i kundens nettverksmiljø.

Programvaredesign

Vårt utrettelige fokus på Xerox® produktsikkerhet begynner tidlig i produktutviklingen med hva som er beste praksis i bransjen for sikker koding, omfattende testing samt analyse for å eliminerer sårbarheter. Xerox® bruker aktivt sertifiseringspraksiser som Common Criteria, og er en aktiv bruker av nye standarder som P2600 Working Group og SDLC (Security Development Lifecycle).

Virkemåte

Xerox® Remote Services foretar følgende operasjoner i et nettverk:

Utrullingsmetode	Applikasjon brukt	Dataflyt i nettverket	Funksjoner anvendt på et nettverk
Device Direct	Ingen	Internt	Xerox®-skriveren forsøker å finne en web-proxyserver (automatisk eller rettet mot en spesifikk adresse)
		Internt	Xerox®-skrivere kan programmeres til å generere anmodninger til en SMTP-server (Simple Mail Transport Protocol) for å sende en varsling på e-post til en definert mottakerliste
		Utenfor nettverket	Xerox®-skriveren når ut gjennom selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Utenfor nettverket	Xerox®-skriveren autentiseres med bruk av sertifikatet overfor den eksterne Xerox-kommunikasjonsserveren før det overføres noen dataattributter
		Utenfor nettverket	Xerox®-skriveren overfører automatisk skriverattributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonsserverne på et angitt tidspunkt daglig, eller når kunden anmoder om det.
		Utenfor nettverket	Xerox®-skriveren sender automatisk en forespørsel til Xerox®-kommunikasjonsserverne gjennom en kryptert kanal (HTTPS over port 443) på et angitt tidspunkt daglig for å få en liste med handlinger som skal utføres (f.eks. sende faktureringsinformasjon nå, legge til en tjeneste osv.)

Utrullingsmetode	Applikasjon brukt	Dataflyt i nettverket	Funksjoner anvendt på et nettverk
		Utenfor nettverket	Enveis on-demand-overføring av tekniske loggdata fra Xerox® Print device gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonsserveren
Device Management-applikasjoner	Centre Ware® Web	Internt	Hver enkelt app forsøker å finne en web-proxyserver (automatisk eller rettet mot en spesifikk adresse)
		Internt	Hver app henter opp skriverfunksjoner for hele maskinparken via SNMP
		Internt	Hver enkelt app henter skriverkonfigurasjoner for hele maskinparken via SNMP
		Internt	Hver enkelt app henter skriverstatus for hele maskinparken via SNMP
		Internt	Hver enkelt app henter data om forbruksartikler for hele maskinparken via SNMP
		Internt	Hver enkelt app kan ta en omstart på en skriver via SNMP eller via skriverens brukergrensesnitt i nettleseren
		Internt	Hver enkelt app kan sende en testside til hver spesifikke skriver
		Internt	Hver enkelt app kan starte opp skriverens nettside
		Eksternt **(bare utgående)**	Hver enkelt app når ut gjennom selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Eksternt**(bare utgående)**	Hver enkelt app autentiseres med bruk av sertifikatet mot den eksterne Xerox-kommunikasjonsserveren før det overføres noen dataattributter
		Eksternt **(bare utgående)**	Hver enkelt app overfører automatisk skriverattributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonsserverne på et angitt tidspunkt hver dag
		Eksternt **(bare utgående)**	Hver enkelt app sender automatisk en forespørsel til Xerox®-kommunikasjonsserverne gjennom en kryptert kanal (HTTPS over port 443) på et angitt tidspunkt hver dag for å få en liste med handlinger som skal utføres
		Internt	Hver enkelt Xerox® Device Agent-app forsøker å finne en web-proxyserver (automatisk eller rettet mot en spesifikk adresse)
		Internt	Hver enkeltXerox® Device Agent-app henter opp skriverfunksjoner for hele maskinparken via SNMP
		Internt	Hver enkelt Xerox® Device Agent-app henter opp skriverkonfigurasjoner for hele maskinparken via SNMP
		Internt	Hver enkelt Xerox® Device Agent-app henter opp skriverstatuser for hele maskinparken via SNMP

Utrullingsmetode	Applikasjon brukt	Dataflyt i nettverket	Funksjoner anvendt på et nettverk
Device Management-applikasjoner	Xerox® Device Agent Partner Edition for overvåkning av skrivere som står i nettverk	Internt	Hver enkelt Xerox® Device Agent-app henter opp data om forbruksartikler for hele maskinparken via SNMP
		Internt	Hver enkelt Xerox® Device Agent-app kan anmode om at enheten skriver ut en konfigurasjonsrapport
		Internt	Hver enkelt Xerox® Device Agent-app kan starte opp en skrivers nettside
		Internt	Hver enkelt Xerox® Device Agent-app kan oppgradere programvaren i en skriver ved å sende en utskriftsjobb. (.DLM-fil over port 9100)
		Eksternt (**bare utgående)**	Hver enkelt Xerox® Device Agent-app når ut gjennom selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Eksternt**(bare utgående)**	Hver enkelt app autentiseres med bruk av sertifikatet mot den eksterne Xerox-kommunikasjonsserveren før det overføres noen dataattributter
		Eksternt **(bare utgående)**	Hver enkelt Xerox® Device Agent-app overfører automatisk skriverattributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonsserverne på et angitt tidspunkt hver dag
		Eksternt **(bare utgående)**	Hver enkelt Xerox® Device Agent-app sender automatisk en forespørsel til Xerox®-kommunikasjonsserverne gjennom en kryptert kanal (HTTPS over port 443) på et angitt tidspunkt hver dag daglig for en liste med handlinger som skal utføres
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper finner en web-proxyserver (automatisk eller rettet mot en spesifikk adresse)
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper henter opp skriverfunksjoner for hele maskinparken via SNMP
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper henter opp skriverkonfigurasjoner for hele maskinparken via SNMP
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper henter opp skriverstatuser for hele maskinparken via SNMP
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper henter opp data om forbruksartikler for hele maskinparken via SNMP
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper kan anmode om at enheten skriver ut en konfigurasjonsrapport

Utrullingsmetode	Applikasjon brukt	Dataflyt i nettverket	Funksjoner anvendt på et nettverk
Device Management-applikasjoner	Xerox® Device Manager for overvåkning av skrivere som står i nettverk	Internt	Xerox® Device Manager / Xerox® Device Agent-apper kan starte opp en skrivers nettside
		Internt	Xerox® Device Manager / Xerox® Device Agent-apper kan oppgradere programvaren i en skriver ved å sende en utskriftsjobb
		Internt	Xerox® Device Manager-appen støtter SNMPv3-kommunikasjon med skrivere
		Internt	Xerox® Device Manager-appen kan foreta endringer i skriverkonfigurasjonen via SNMP og webgrensesnittet
		Internt	Xerox® Device Manager-appen henter jobb-baserte regnskapslogger fra visse Xerox®-multifunksjonsskrivere
		Internt	Xerox® Device Manager-appen administrerer/gjennomtvinger kontrollpolicyer
		Eksternt **(bare utgående)**	Xerox® Device Manager / Xerox® Device Agent-appene når ut gjennom selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Eksternt**(bare utgående)**	Hver enkelt app autentiseres med bruk av sertifikatet mot den eksterne Xerox-kommunikasjonsserveren før det overføres noen dataattributter
		Eksternt **(bare utgående)**	Xerox® Device Manager / Xerox® Device Agent-appene sender automatisk data om skriveren til Xerox®-kommunikasjonsserverne gjennom en kryptert kanal (HTTPS over port 443) på et angitt tidspunkt hver dag
		Eksternt **(bare utgående)**	Xerox® Device Manager / Xerox® Device Agent-appene sender automatisk en forespørsel til Xerox®-kommunikasjonsserverne gjennom en kryptert kanal (HTTPS over port 443) på et angitt tidspunkt hver dag for å få en liste med handlinger som skal utføres

SNMP (Simple Network Management Protocol)

SNMP (Simple Network Management Protocol) er det mest utbredte verktøyet for styring av å kommunikasjon mellom administrasjonssystemer for nettverk og nettverksskrivere. Device Management-applikasjoner bruker SNMP i søk for å hente detaljert informasjon om skriveren i nettverket. Xerox Device Management-applikasjoner støtter SNMP v1/v2 og v3-protokoller. I sertifiseringsveiledningene til Xerox® Device Management-applikasjonen finner du mer detaljert informasjon.

SNMP v3-rammeverket støtter flere sikkerhetsmodeller som kan eksistere samtidig innenfor en SNMP-entitet. SNMPv3 inkluderer strengere sikkerhet ved å tilføye kryptering til SNMP2. I tillegg er SNMPv3 bakoverkompatibel med tidligere versjoner og er utbredt i robuste nettverk.

Xerox® Device Management-applikasjoner (Centre Ware® Web / Xerox® Device Manager) kan kommunisere med maskinplattformer som følger FIPS 140-2 i implementeringen av SNMPv3.

Xerox Device Management-applikasjoner bruker ikke Windows SNMP-tjenesten eller Windows SNMP Trap-tjenesten. Hvis disse tjenestene allerede er installert på en datamaskin (PC) eller en server som har Xerox® Device Management-applikasjonen, **må** tjenestene deaktiveres først.

Xerox® Device Management-applikasjoner benytter en SNMP-agent utviklet av Xerox, som:

- inneholder en spesielle kodings-/dekodingsmekanisme
- er helt .NET-styrt
- bruker .NET runtime.exe-fil som gir økt sikkerhet ved å hindre angrep mot sårbarheter i programvaren, slik som ugyldig manipulering av pekere, bufferoverskridelse og bound checking.

Xerox® Device Management-applikasjonene utnytter sikkerhetsfunksjonene som er tilgjengelige i Windows (operativsystemet), inkludert:

- brukerautentisering og godkjenning
- konfigurasjon og styring av tjenester
- utrulling og administrasjon av gruppepolicy

ICF (Windows Internet Connection Firewall) inkludert:

- innstillinger for sikkerhetslogging
- ICMP-innstillinger

Xerox® Device Management-applikasjoner: **Xerox® Device Agent, Xerox® Device Agent Partner Edition og Xerox® Device Manager** bruker SQL CE-applikasjon Microsoft® SQL Server

Xerox® Device Management-applikasjonen kan konfigureres slik at den utnytter de ekstra sikkerhetsfunksjonene som finnes i Microsoft® SQL Server-applikasjonen, inkludert:

- aktivering av brukerkontoregistrering

- kryptering av DNS (Domain Name System)
- begrensning av kontorettigheter i databasen (dvs. eierrettigheter)
- iverksetting av brukerdefinerte portnumre

Det kreves en Xerox-registreringsnøkkel og en gyldig Xerox-konto for å overføre data til de eksterne Xerox®-kommunikasjonsserverne.

Den eksterne kommunikasjonen som Xerox® Device Management-applikasjonene utfører, kan påvirkes av Windows-brannmuren. (Vi **anbefaler** at kundene hvitlister Xerox-URLen i brannmuren og spesifiserer IP-adressen som skal ha tilgang til URLen.)

Xerox® Device Management-applikasjonene kjører i bakgrunnen og bruker lokale systemrettigheter til automatisk å kontakte nettverksskrivere via SNMP og periodisk overføre skriverattributter tilbake til Xerox®-kommunikasjonsserverne

Tilgangen til Xerox® Device Manager (XDM)-applikasjonens brukergrensesnitt (UI) og funksjoner styres via følgende rollebaserte privilegier (f.eks. Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators og Centre Ware® Web Customers).

Brukernavn og passord for applikasjonene sendes ikke over nettverket. I stedet blir det benyttet adgangssymboler (iht. Windows® OS-design).

Xerox® Device Manager (XDM)-applikasjonen har kontrollbasert sikkerhet for utskrifter som begrenser jobber iht. policy når det gjelder bruk av farger, dokumenttype, jobbkostnad, tidspunkt på dagen, adgangskontroll for brukergruppen, policy for tosidig utskrift, tillatte trykkjobber og utskriftskvoter.

Merknader: Bruken av SNMP i en Xerox® Remote Services-applikasjon skal ikke utgjøre en sikkerhetsrisiko i kundens IT-miljø, fordi all SNMP-basert trafikk som disse applikasjonene genererer eller forbruker, skjer i kundens intranett bak brannmuren. Windows SNMP-tjenesten og Windows SNMP Trap-tjenesten er ikke aktivert i Windows (operativsystemet) som standard.

Corporation Security-modus

I tillegg til enhver planlagt synkronisering mellom Xerox® Device Management-applikasjonene og Xerox® Service manager, foretas det en daglig synkronisering som standard. De to eksisterende Corporation Security-modusene er **Normal** og **Låst .**

I **Normal** modus kontakter Device Management-applikasjonen Xerox® Services Manager daglig når alle andre planlagte synkroniseringer er blitt slått av (***anbefalt modus***).

I **Låst** modus er det ingen kommunikasjon med Xerox® Services Manager, bortsett fra skriverrelatert datasynkronisering. Endringer av denne innstillingen må gjøres fysisk på stedet. (***Datasynkronisering*** sikrer at skriverinformasjonen som sendes fra Xerox® Device Management-applikasjonen, og det som fanges opp i Xerox® Services Manager, er den samme.)

Standardinnstillingen er at Xerox® Device Management-applikasjonen kontakter Xerox® Services Manager daglig, og gjør det mulig for administratorer å endre innstillingene eksternt slik at besøk på stedet unngås. Vi anbefaler at denne innstillingen ikke endres. Hvis en kunde begrenser Xerox-personellets mulighet til å foreta service på skrivere eksternt, kan maskinens kommunikasjon med Xerox® Services Manager låses med unntak for synkronisering av skriverdata. I denne modusen rapporterer ikke lenger applikasjonen innstillingene til en datamaskin, skriver, IP-adresse eller lokasjon til Xerox® Services Manager, og alle endringer av innstillingene krever et fysisk besøk på stedet.

Merk: Hvis Xerox® Device Agent ikke har fanen Corporation Security Mode, kjører den i Normal modus.

Protokoller, porter og andre beslektede teknologier

Den følgende tabellen viser hvilke protokoller, porter og teknologier som benyttes i Xerox® Remote Services:

Portnummer	Protokoll	Beskrivelse av bruk	Dataflyt i nettverket
Avhengig av øvre lags protokoller	**Internettprotokoll (IP)**	**Underliggende transport for all datakommunikasjon**	**Internt + eksternt (bare utgående)**
Ikke relevant	ICMP (Internet Control Message Protocol)	Søk etter skriver + feilsøking	Internt
25	SMTP (Simple Mail Transport Protocol)	Skriver + e-postvarsling om Remote Proxy-app	Internt
53	DNS (Domain Name Services)	Benyttes til DNS-baserte søk etter skriver	Internt
80	HTTP (Hyper Text Transport Protocol)	Spørring fra nettside til skriver + spørring fra nettside til Device Management-applikasjon	Internt
135	RPC (Remote Procedure Call)	Søke etter skriver	Internt
137, 139	NetBIOS	Søk etter skriverserver	Internt
161	SNMP (Simple Network Management Protocol) v1 / v2c / v3	Standard protokoll som brukes til å søke etter skrivere i nettverket + Hent-status, tellere og data om forbruksartikler + Hent og bruk enhetskonfigurasjon. Standard gruppenavn = «public» (GET), «private» (SET)	Internt
162	SNMP traps	Standard gruppenavn = «SNMP_trap»	Internt
389	LDAP (Lightweight Direct Access Protocol)	Søke etter skriver via MS Active Directory-liste + Konfigurasjonspakke for skannetjenesten + Active Directory-kundeimport + Innstillinger for kundegruppe	Internt
443	HTTPS (Hyper Text Transport Protocol Secure)	Søk fra sikker nettside etter skriver (hvis konfigurert) + søk fra sikker nettside etter Remote Proxy-app (hvis konfigurert) + Overføring av skriverdata tilbake til Xerox®-kommunikasjonsserverne + informasjon om skriverkontrollene tilbake til Xerox® Device Manager	Internt + eksternt (bare utgående)
452	Netware SAP (Service Advertising Protocol)	Søk etter skriver med bruk av Novell Server-spørring via IPX	Internt

Portnummer	Protokoll	Beskrivelse av bruk	Dataflyt i nettverket
515, 9100, 2000, 2105	Sending av utskriftsjobb via TCP/IP og Raw Port	Oppdatering av skriverens programvare + Diagnostikk av testutskriftsside	Internt
631	IPP (Internet Printing Protocol)	Søke etter skriver	Internt

Sikkerhet – beste praksis

Hold alltid skrivere oppdatert med nyeste fastvare/programvare. Bruk enten skriverens webgrensesnitt (UI) eller skriverens kontrollapplikasjon fra Xerox® og andre leverandører for å oppgradere skriverens fastvare/programvare.

Deaktiver ubrukte skriverporter og protokoller på skriveren der det er mulig. Dette gjøres typisk i webgrensesnittet (UI) på kontorskrivere, og med lokalt brukergrensesnitt (UI) på produksjonsskrivere.

Bruk funksjoner som begrenser brukeradgangen til skrivere, der dette er tilgjengelig. Dette gjøres typisk i webgrensesnittet (UI) på kontorskrivere, og med lokalt brukergrensesnitt (UI) på produksjonsskrivere.

Bruk sikre protokoller der dette er mulig. Dette gjøres typisk i webgrensesnittet (UI) på kontorskrivere, og med lokalt brukergrensesnitt (UI) på produksjonsskrivere.

Aktiver sikkerhetsfunksjoner som er integrert i enheten (f.eks. bilde-overskriving, diskkryptering, sikker utskrift osv.)

Sørg for at virksomhetens brannmur kan rute HTTPS-pakker gjennom port 443 iht. corporate security-policyer.