Fjerntjenester hos Xerox

Tekniske dokumenter om sikkerhet

Versjon 4.0

Mars 2022

IS 614672/IS 514590

Innholdsfortegnelse

1. Generelt formål og publikum

De tekniske dokumentene om sikkerhet for fjerntjenester hos Xerox inkluderes for å hjelpe kunder å forstå og bruke den sikre fjerntjenesteløsningen som fungerer best med deres nettverkkonstruksjon- og informasjonsikkerhetsretningslinjer. or å garantere den sikreste konfigurasjonmetoden merk at endringer på kundens Internett-brannmur, nettproksyservere eller andre sikkerhetsrelatert nettverkinfrastruktur kan være nødvendig.

Målpublikum for dette dokumentet inkluderer tekniske selgere, nettverkledere og nettverksikkerhetsfagfolk som er interessert i fjerntjenestefunksjoner og sikkerhetsimplementeringen til disse funksjonene.

Vi anbefaler at dokumentet gjennomgås i sin helhet for å sertifisere bruken av Xerox® produkter og tjenester innenfor en kundes nettverkmiljø.

2. Verdiforslag

Vi tilbyr en trygg og sikker måte for å sende enhetdata til vårt ISO-sertifiserte system for å automatisere vanlige oppgaver og gir en bedre service- og supportopplevelse.

- Faktureringsmålingsrapportering er automatisert og nøyaktig.
- Programmet for automatisk påfylling av forbruksvarer forsyner blekk basert på de rapporterte blekknivåene til skriveren, slik at det ikke er noe behov for å spore inventar eller ringe etter forsyninger.
- Sending av diagnostisk informasjon gjør at vi lettere kan støtte enheten, ofte ved å aktivere en hurtigere problemløsning.
- Visse skrivermodeller kan sjekke etter viktige programvareoppdateringer og installere oppdateringene programmessig uten kundens intervensjon.Se merknad
- Våre administrerte serviceegenskaper gir også en måte å administrere skrivere av andre merker enn Xerox i tillegg til skrivere av merket Xerox.
- Disse tjenestene vil gjøre en kunde i stand til mer effektiv bruk av sin tid.

Alt dette gjøres med sikkerheten i tankene.

Merk: Dette alternativet kan deaktiveres for miljøer der kunder sertifiseres for en bestemt programvareversjon og ønsker å kontrollere utskriftprogramvaren når det skjer oppdateringer. Dette kan gjøres uten å måtte deaktivere resterende fjerntjenesteegenskaper.

3. Fjerntjenester

Informasjon er en viktig verdi, og sikkerhet er avgjørende for alle organisasjonaktiva, inkludert nettverkbaserte multifunksjonutskriftenheter (MFP-er). I dag medfører administrasjon av en flåte av multifunksjonutskriftenheter, samtidig som det garanteres et akseptabelt nivå av sikkerhet, et sett av unike utfordringer som ofte overses. Vi forstår fullstendig denne kompleksiteten og er responsive overfor våre kunders sikkerhetsbehov. Xerox®-produkter, Xerox®-systemer og fjerntjenestetilbud er designet til å sikkert integrere med våre kunders eksisterende arbeidsflyter, samtidig som de nyeste sikre teknologiene brukes.

Som standard overføres ingen kundebilder fra utskrift-, faks-, skanne-, kopieringsinformasjon eller annen sensitiv informasjon til våre servere.

De USA-baserte Xerox-serverne oppfyller strenge sikkerhetskrav for informasjonsikkerhetsadministrasjon. Våre datasentre og fjerntjenesteapplikasjoner opprettholder den årlige Statement on Standards for Attestation (SSAE) nr. 16, Sarbanes-Oxley Act (SOX) samsvarskrav og er ISO 27001:2013-sertifisert.

4. Brukmodeller

Kunder kan velge mellom følgende tilsvarende sikre Xerox® fjerntjenestebrukmodeller:

- **Kombinasjonmodellen** –***(foretrukket modell)*** Implementeringen av både Device Direct- og Device Management Application-modellen sammen er ideell, da den gir det mest robuste datasettet og enhetadministrasjon-funksjonene.

- **Device Direct-modellen** - Device Direct gjør det mulig for utskriftenheter å kommunisere direkte med fjern-Xerox®-kommunikasjonservere via Internett gjennom kundens brannmur for å støtte automatiske forsyningspåfyllinger (ASR), automatiske måleravlesinger (AMR) og enhetdiagnostisk rapportering. Denne brukmodellen gir et sett av dataelementer i standard belastning for å inkludere enhetfeil, varslinger, tellere, High Frequency Service Items (HFSI) og andre utskriftenhetattributter.
- **Device Management Applicaton-modellen** - Xerox®-enhetadministrasjonapplikasjoner kan brukes i en kundes nettverk for innhente et sett av dataattributter fra utskriftenheter for å også støtte automatiske forsyningspåfyllinger (ASR), automatiske måleravlesinger (AMR) og enhetdiagnostisk rapportering. Utskriftenhetattributter er innhentet og deretter overført på sikker måte til fjern-Xerox-servere. Dataattributter fra både Xerox-skrivere og andre skriverenheter kan kommuniseres som en del av denne brukmodellen.

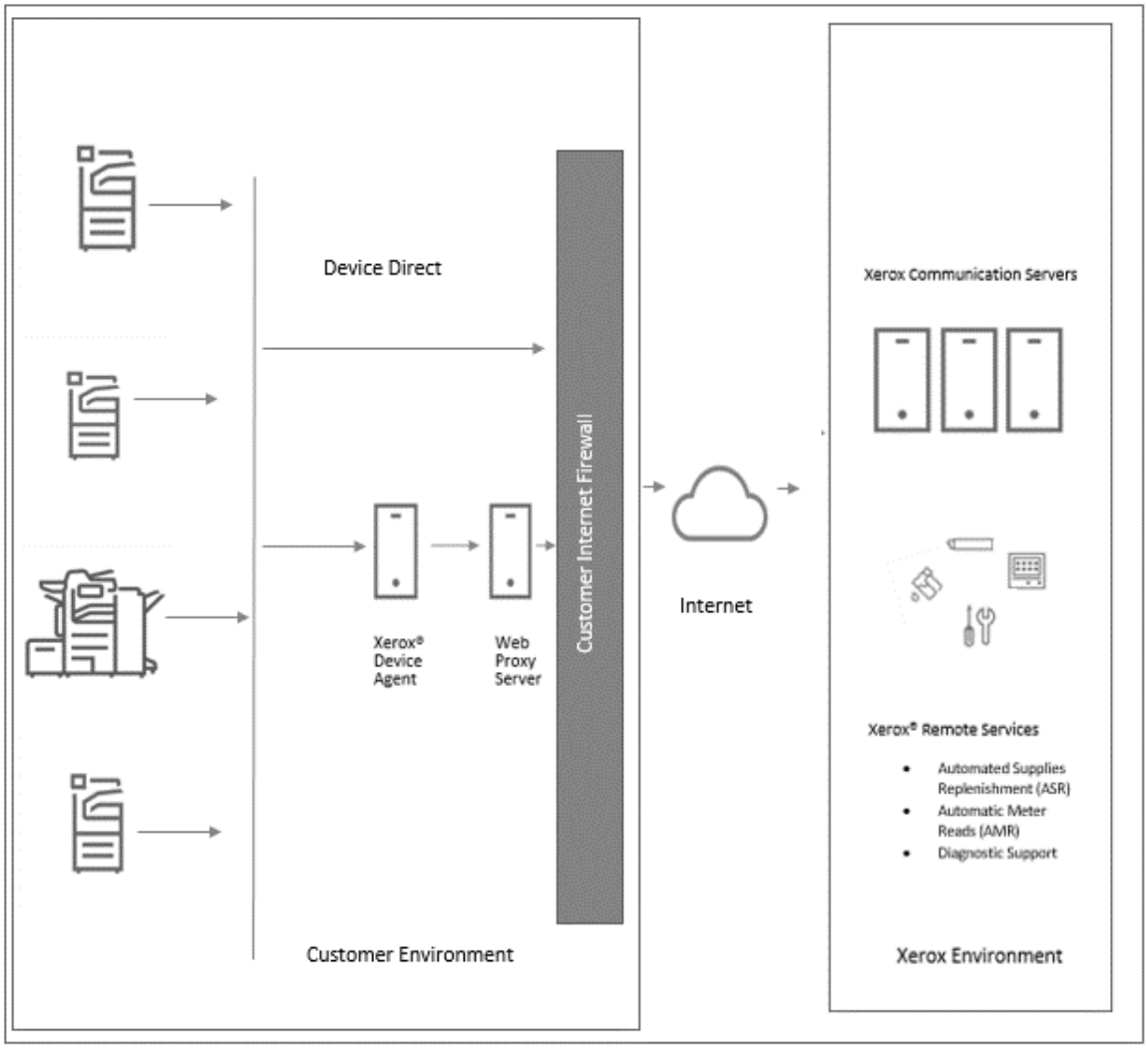
Alle brukmodeller for Xerox®-fjerntjenester er like sikre og utnytter den siste bransjestandarden for nettbaserte protokoller og porter for å opprette en sikker, kryptert kanal ved overføring av utskriftenhetattributter eksternt til fjern-Xerox-servere som finnes innenfor våre redundant sikrede datasentre.

Brukmodellen som er valgt, avhenger av våre kunders type utskrifttjenesteløsning, inform-asjonsikkerhetsretningslinjer og regler for å håndtere overføringen av utskriftenhetdataattributter.

Kombinasjonbrukmodell (foretrukket)

Kombinasjonbruk er brukt når en kunde kjøper flere typer av Xerox vedlikeholdsavtaler for utskriftenhetene og for å oppnå en mer robust fjerntjenesteløsning. Når en Xerox®-utskriftenhet er installert på et nettverk første gang, er standard Xerox-fjerntjenesters atferd for utskriftenheten å automatisk forsøke å kommunisere utgående til våre kommunikasjonservere ved bruk av en sikker, autentisert tilkoblingsmetode.

Figur 1



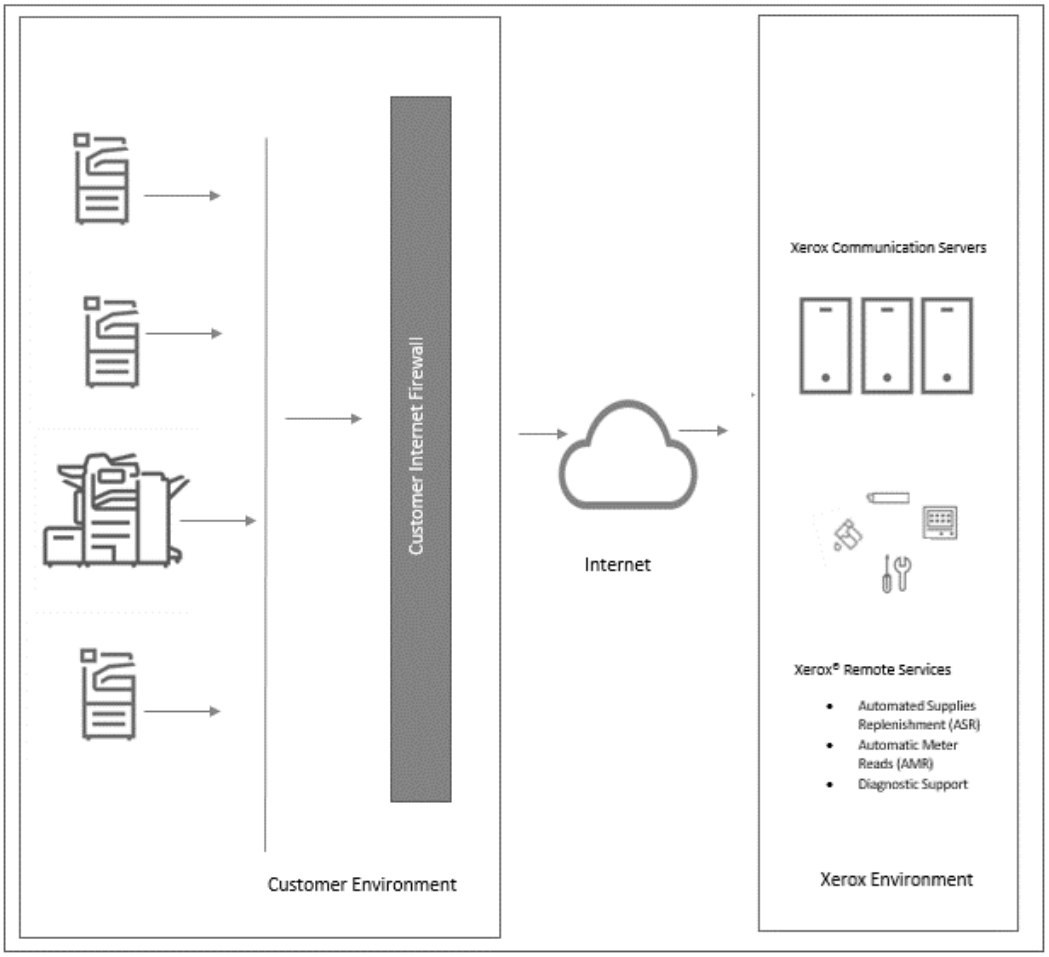
Combination Deployment Model

Device Direct-brukmodellen

Fjerntjenestekompatible Xerox®-enheter bruker en TLS (Transport Layer Security) 1.2-protokoll-tilkobling via den sikre standardporten 443 for å kommunisere utgående til våre sikre servere.

- Utskriftenheter innenfor kundens miljø initierer all kommunikasjon med kommunikasjonserverne. Standard brannmurkonfigurasjoner på stedet må aktivere kommunikasjon.
- En gyldig URL for kommunikasjonserverne må brukes (*.xerox.support.com) for å autentisere utskriftenheter til Xerox-infrastrukturen.
- Enheten forespør en registrering med kommunikasjonserverne ved bruk av sertifikatautentiseringsegnede innloggingsopplysninger.
- Kommunikasjonserverene validerer innloggingsopplysningene som leveres av skriverne og godtar forespørslene.
- Kommunikasjonserverne er bak en sikker brannmur og er ikke tilgjengelige fra Internett.

Figur 2



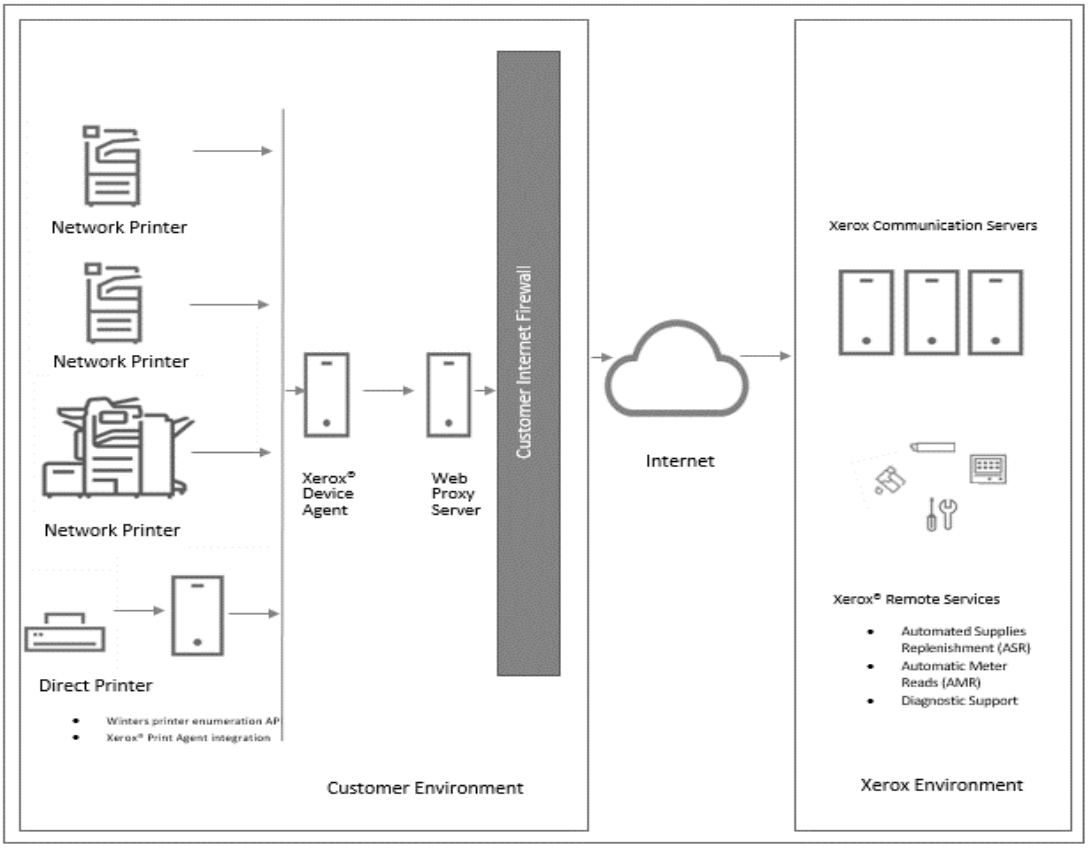
Device Direct Deployment Model

Enhetadministrasjonprogram-brukmodellen

Enhetadministrasjonapplikasjoner (dvs. **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition og Xerox Device Manager)** bruker en TLS (Transport Layer Security) 1.2-protokoll over den sikre standardporten 443 til å kommunisere eksternt til kommunikasjonserverne. Ytterligere funksjoner er utnyttet for å forbedre sikkerheten over denne kanalen og er etablert i løpet av den innledende installasjonen av enhetadministrasjonapplikasjoner, som inkluderer:

- Enhetadministrasjonapplikasjonen innenfor kundens miljø initierer all kommunikasjon med kommunikasjonserverne. Standard brannmurkonfigurasjoner på stedet må aktivere kommunikasjon.
- Kommunikasjonserverne er bak en sikker brannmur og er ikke tilgjengelige fra Internett.
- Enhetadministrasjonapplikasjonen forespør en registrering med fjernserverne ved bruk av sertifikatautentiseringsegnede innloggingsopplysninger.
- Kommunikasjonserverne validerer innloggingsopplysningene som leveres av skriverne og godtar forespørslene.
- Enhetadministrasjonapplikasjonen autentiserer kommunikasjonserverne og aktiverer tjenesten.

Figur 3



Device Management Application Deployment Model

5. Dataoverføring og nyttelast

Datakilder

Utskriftenhetdataattributter som sendes som en del av overført nyttelast, er fra følgende kilder:

- Xerox® Office nettverkskrivere
- Andre nettverkskrivere enn de fra Xerox
- Xerox®-produksjonskrivere
- Xerox®-enhetadministrasjonapplikasjoner

Merk: Ikke alle Xerox kontor- og Xerox produksjonskrivere er kompatible med Xerox-fjerntjenester. Du finner en fullstendig liste over kompatible produkter her. Utskriftenhetattributter varierer etter produkt og Xerox®-fjerntjenestebrukløsning.

Xerox® Office-enheter

Tabell 1 Identifiserer enhetdataattributtene som kan overføres for fjerntjenestekompatible Xerox®-kontorprodukter.

Dataattributter	Detaljert beskrivelse av dataattributter
Utskriftenhe-tidentitet	Inkluderer modell, modellfastvarenivåer, modulserienumre, modulinstallasjondatoer, lisensdata og plassering, hvis tilgjengelig.
Utskriftenhetens nettverkadresse	Inkluderer Media Access Control (MAC)-adresse, subnettadresse.
Utskriftenhet-egenskaper	Inkluderer detaljert maskinvarekomponentkonfigurasjon, detaljert programvaremodulkonfigurasjon, funksjoner/tjenester som støttes osv.
Utskriftenhet-status	Inkluderer aktive statuser, feilhistorikktellinger, DFE-hendelselogg, dataoverføringshistorikk
Utskriftenhet-tellere	Inkluderer faktureringsmålere, utskriftrelaterte tellere, kopirelaterte tellere, storjobb-relaterte tellere, produksjonspesifikke tellere, skann-til-destinasjon-relaterte tellere på modeller med lav sluttproduksjon.
Utskriftenhet-forbruksvarer	Inkluderer produsent, modell, serienummer, navn, type, nivå, kapasitet, status, livslange tellere osv.
Utskriftdetaljert maskinbruk	Inkluderer HFSI-data, NVM-data, deleutskiftning, DFE-logger, detaljerte diagnostiske data, feiloppløsning.
Teknisk / utbedring av små program-meringsfeil	Inkluderer ikke-strukturerte, detaljerte data relatert til utbedring av små programmeringsfeil, beregnet til bruk kun for 3. nivå support.
Kundejobb-relatert	Xerox®-produksjonutskriftprodukter gir muligheten til å reprodusere jobbrelaterte data i støtte av eskalerte støttescenarioer via kryptert PostScript til Xerox. Kunden kan kontrollere om denne funksjonen skal aktiveres eller ikke. Hvis kunden velger å overføre jobbrelaterte data (dvs. kryptert PostScript) tilbake til Xerox, håndteres disse dataene i samsvar med Xerox-informasjonsikkerhetsretningslinjer (IS) og standarder.

Våre utskriftenheter i kontorklassen overfører enhetdataattributter i et eXtensible Markup Language (XML)-format ved bruk av en komprimert .zip-fil. Etter autentiseringen overføres hver fil deretter via en kryptert kanal til kommunikasjonserverne.

Xerox® produksjonenheter

Tabell 2 Identifiserer enhetdataattributtene som kan overføres for fjerntjenestekompatible Xerox®-produksjonprodukter.

	Beskrivelse
Utskriftenhetidentitet	Inkluderer modell, fastvarenivå, modulserienumre og installasjondata.
Utskriftenhetens nettverkadresse	Inkluderer Media Access Control (MAC)-adresse, subnettadresse.
Utskriftenhet-egenskaper	Inkluderer detaljert maskinvarekomponentkonfigurasjon, detaljert programvaremodulkonfigurasjon, funksjoner/tjenester som støttes, strømsparingsmoduser, osv.
Utskriftenhetstatus	Inkluderer helhetlig status, detaljerte varslinger, de siste 40 feilhistorikk, fastkjøringsdata, osv.
Utskriftenhettellere	Inkluderer faktureringsmålere, utskriftrelaterte tellere, kopirelaterte tellere, faksrelaterte tellere, storjobb-relaterte tellere, skann-til-destinasjon-relaterte tellere, brukstatistikk, osv.
Utskriftenhetforbruksvarer	Inkluderer forbruksvarenavn, type (dvs. avbildning, finishing, papirmedier), nivå, kapasitet, status, størrelse, osv.
Detaljert utskrift av maskinbruk	Inkluderer detaljerte utskriftrelaterte tellere, innkoblingstatuser, detaljerte CRU (Customer Replaceable Units)-enheter utskiftningsantall, detaljert CRU-feildata og distribusjoner, integrert OCR (Optical Character Recognition)-funksjonbruk, utskriftomgangslengde distribusjon, papirskuffbrukdistribusjon, installerte medier, medietypedistribusjon, mediestørrelsedistribusjon, dokumentlengdedistribusjon, sett-nummer, HFSI-data, NVM-data, distribusjon, merkede pikseltellinger, gjennomsnittlig områdedekning per farge, feil/fastkjøringer, detaljerte skanningsrelaterte tellere.
Teknisk / utbedring av små programmeringsfeil	Inkluderer detaljert informasjon for løsning av små feil, som kan inkludere data utenfor datasettet som er opplistet ovenfor. Disse dataene kan inkludere PII, slik som brukernavn, e-postadresser og jobbdata. Disse dataene er kun sendt med uttrykt tillatelse fra kunden og er beregnet kun til bruk til eskalert feilsøkingssupport.

Våre utskriftenheter i produksjonklassen overfører enhetdataattributter i et eXtensible Markup Language (XML)-format ved bruk av en komprimert .zip-fil. Etter autentiseringen overføres hver fil deretter via en kryptert kanal til fjerntjenesteserverne.

Merk: Filen og innholdet av dataene som er identifisert varierer etter produktmodell.

Xerox®-enhetadministrasjonapplikasjoner

Det finnes flere alternativer for enhetadministrasjonapplikasjoner som er tilgjengelige basert på kundens nettverkmiljø og utskriftenhetadministrasjonbehov. Alle er like sikre og har robuste utskriftenhetadministrasjonegenskaper.

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

Hver applikasjon synkroniserer som standard minst daglig med de sikre kommunikasjonserverne. For å sikre maksimal sikkerhet for dine data, er kommunikasjonserverne plassert i en ISO 27001-kompatibel fasilitet. Data som er sendt er primært skriverspesifikke faktureringstellere, forsyningsnivåer og skrivervarslinger. Data komprimeres, krypteres og beskyttes av flere mekanismer:

- Xerox Device Management Application initierer all kontakt med Xerox-kommunikasjonservere, standard brannmurkonfigurasjoner i kundens miljø kreves for å aktivere kommunikasjon.
- Xerox Device Management Applications krever en gyldig proksy, i tilfelle en proksy kreves for Internett-kommunikasjon.
- Xerox-kommunikasjonserverne finnes bak en sikker brannmur i Xerox-miljøet og er ikke tilgjengelige fra Internett.
- Xerox-kommunikasjonserverens brukergrensesnitt krever autentisering. Xerox Device Management Applications vertinformasjon lagres i en konto som er spesifikk for kundens anlegg, og tilgangen til disse kontodataene i Xerox-kommunikasjonservere er begrenset til kontoadministratorer for Xerox-kommunikasjonservere.
- All kommunikasjon til Xerox-kommunikasjonserveren logges og er tilgjengelig for visning.
- Data som sendes til dine nettverktilkoblede utskriftenheter, hvis aktivert, består primært av fjerne kommandoer som gjør det mulig for en kontosupportadministrator å forespørre Xerox Device Management Application-kommandonivåutførelse i løpet av eskalerte supportscenarioer.
- Forespørsler involverer hovedsakelig fastvareoppdateringer, omstart av skriveren, utskrift av testside og gjeldende enhetstatusoppdateringer.
- Xerox Device Management Application forespør regelmessig sine Xerox-kommunikasjonserverkontoer for kommandoforespørsler.
- Operasjoner er resultatet av kommandoforespørsler som sendes til Xerox-kommunikasjonserverne, der de deretter gjennomgås.

Merk: Det er et engangsregistreringskrav ved programvareinstallasjon. Denne registreringsinformasjonen inkluderer et felt for enhetplassering og kontakt-e-post.

Xerox Device Management Applications **(dvs. Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition og Xerox Device Manager)** overfører utskriftattributtdataene i eXtensible Markup Language (XML)-format ved bruk av en komprimert .zip-fil. Filen krypteres deretter og overfører til fjernkommunikasjonservere via krypterte kanaler.

Tabell 3 Identifiserer en liste over enhetdataattributter og beskrivelse som kan sendes via Xerox® Device Mgmt.-appen.

Dataattributter	Detaljert beskrivelse av dataattributter
Utskriftenhetidentitet	Inkluderer produsent, modell, beskrivelse, fastvarenivå, serienummer, aktivatagger, systemnavn, kontakt, posisjon, administrasjonstatusarbeidsstasjon (skrivebord), fakstelefonnummer og kønavn.
Utskriftenhetens nettverkadresse	Inkluderer MAC-adresse, IP-adresse, DNS-navn, subnettmaske, IP standard gateway, sist kjente IP-adresse, IP-adresse endret, tidssone, IPX-adresse, IPX eksternt nettverknummer, IPX utskriftserver.
Utskriftenhet-egenskaper	Inkluderer komponenter som er installert, komponentbeskrivelser, støttede funksjoner/tjenester, utskrifthastighet, fargesupport, fullføringsalternativer, dupleksstøtte, markedsføringsteknologi, harddisk, RAM, språkstøtte, brukerdefinerte egenskaper.
Utskriftenhetstatus	Inkluderer helhetlig status, detaljerte varslinger, lokale konsollmeldinger, komponentstatus, status gjenhentingsrelaterte data, oppdagelsedato, oppdagelsemetode/-type, enhetens drifttid, feller støttede/aktiverte.
Utskriftenhettellere	Inkluderer faktureringsmålere, utskriftrelaterte tellere, kopirelaterte tellere, faksrelaterte tellere, storjobb-relaterte tellere, skanning-relaterte tellere, brukstatistikk og målvolum.
Utskriftenhet-forbruksvarer	Inkluderer forbruksvarenavn, type (dvs. avbildning, finishing, papirmedier), nivå, kapasitet, status, størrelse og relaterte attributter.
Utskriftenhet, detaljert bruk	Brukerbasert jobbsporingsdata, som inkluderer jobbkarakteristikk (ID, dokumentnavn, eier, dokumenttype, jobbtype, farge, dupleks, nødvendige medier, størrelse, sider, sett, feil), destinasjon (utskriftenhet, modell, DNS-navn, IP-adresse, MAC-adresse, serienummer), resultat er utskrift av jobben (innleveringstid, jobbutskrifttid, utskrevne sider, sider utskrevet i farge / svart/hvitt, fargemodus brukt, N-up), regnskapsdata (chargeback-kode, chargeback-pris, regnskapkilde), kilde for utskriftjobb (arbeidsstasjon, utskriftservernavn/MAC-adresse, kønavn, port, brukernavn, bruker-ID), Xerox-administrasjondata (sendt til Xerox Services Manager).
Enhetbehandling-sidentitet	Inkluderer applikasjonvert-PC-informasjon, slik som DNS-navn, IP-adresse, OS-navn, OS-type, PC, CPU, RAM-størrelser (ledig kontra brukt), harddiskstørrelser (ledig kontra brukt), stedsnavn, appversjon, utløpsdato for applisens, .Net-versjon, tidssone, oppdagelse-komponentversjon, hoveddatabasestørrelse, oppdagelse-databasestørrelse, antall skrivere / innenfor omfang / utenfor omfang, kritiske tjenester i drift.
Enhetbehandler selskap-sikkerhetsmodus	Normal modus = Xerox Device Agent kontakter Xerox Services Manager, daglig. Innstillinger kan endres fjernt uten behov for besøk på stedet, selv når forespørselplaner er slått av. Avsperringsmodus = unntatt skriverrelatert datasynkronisering er det ingen kommunikasjon med Xerox Services Manager, og innstillinger må endres på stedet. Xerox Device Agent-maskins og -skrivers IP-adresser er rapportert til Xerox Service Manager.
Enhetadmini-strasjonens utskrift-kontrollretningslinjer	Inkluderer sluttbruker-PC-navn, utskriftserver som er brukt, utskriftkø som er brukt, tidsstempel for overtredelse, dokumentnavn, sluttbrukers brukernavn, jobbdupleks, jobbfarge, totale inntrykk av jobb, jobbpris, tiltak tatt, sluttbruker varslet, melding vist, utskriftretningslinjenavn, regel for utskriftretningslinjer.

6. Fjern administrasjon av utskriftenheter

Xerox-eskalert supportpersonale kan behandle følgende tiltak gjennom Device Direct eller Xerox Device Management Application.

Tabell 4 viser forbedrede oppløsningsinnsatser, tillatt av kunden i et eskalert supportscenario. Tillatelse fra kunden til å utføre disse funksjonene må uttrykkelig innhentes.

Data	Beskrivelse
Handlinger som skal utføres på utskriftenheter	• Hent enhetstatus = hent inn siste status fra utskriftenheten • Omstart enhet = initier en avstengnings-/oppstartsekvens på utskriftenheten • Oppgrader enhet = installer ny programvare/fastvare på utskriftenhet (DLM over port 9100) • Feilsøk enhet = ping enhet + hent inn siste status fra utskriftenheten • Skriv ut testside = send inn en testjobb til en utskriftenhet for å validere utskriftbanen (generer en konfigurasjonrapport) • Start administrasjonenhet = initier periodisk utskriftenhet dataoverføringer til eksterne Xerox®-kommunikasjonservere **Merk**: **Hvert tiltak kan deaktiveres fra bruk på forespørsel innenfor administrasjonkonfigurasjondelen til Xerox®-enhetadministrasjonapplikasjoner som støtter denne funksjonen.**
Handlinger som skal utføres på enhetadministrasjonapplikasjoner	Innstillinger innenfor hver enhetadministrasjonapplikasjon som kan håndteres, inkluderer oppdagelseoperasjon, dataeksportfrekvens, SNMP-kommunikasjonrelaterte innstillinger (prøv på nytt, tidsavbrudd, miljønavn), varslingsprofiler og automatisk programvareoppdateringsfrekvens for enhetadministrasjonapplikasjonen.
Fjern programvare-administrasjon	Visse enheter er utstyrt med automatiske fjernprogramvareadministrasjonfunksjoner. Disse enhetene sender en forespørsel til Xerox-miljøet for å se om det finnes noen tilgjengelige nye programvareoppdateringer for enheten. Hvis det finnes noen, vil enheten være i stand til å deretter sende en forespørsel for denne programvareoppdateringen, og den vil bli oppdatert ved foreskrevet tid. Men hvis miljøet forbyr automatiske programvareoppdateringer kan fjernprogramvareadministrasjonalternativet kun fravelges uten avbrudd av standard fjerntjenester.

Systemkrav for enhetadministrasjonapplikasjoner

Minimumskrav varierer lett i henhold til tilbud. Se brukerhåndboken, sikkerhetevalueringsguiden og/eller sertifiseringsguiden for baselinjekrav som er spesifikke for de respektive enhetadministrasjonapplikasjonene.

Ved installasjon er en readme-fil inkludert for å håndtere ekstra og spesifikke systemkrav for den respektive enhetadministrasjonapplikasjonen som installeres.

- Enhetadministrasjonapplikasjonene er kompatible med sikkerhetsfunksjonene som er integrert i Windows®-operativsystemet. De er støttet på en bakgrunns-Windows®-tjeneste som kjører under de lokale systemkontoopplysningene for å aktivere proaktiv overvåkning av skrivere og utskriftdataattributtlasten som vil bli overført til Xerox. Brukergrensesnittet som viser utskriftdataattributtlasten er kun tilgjengelig for strømbrukere og administratorer med tilgang til Windows® OS.

- For å forhindre et avbrudd av automatisk fjerntjenestekommunikasjon, anbefales det at enhetadministrasjonapplikasjonen lastes på en klient som strømforsynes kontinuerlig eller i løpet av kjerneforretningtiden.

- Vi anbefaler at vertdatamaskiner kjører et støttet operativsystem fra Microsoft® Corporation. Men Xerox Device Management-applikasjoner kan kjøres på Apple® OS 10.9.4 eller senere ved bruk av Parallels Desktop emulasjonprogramvare. Applikasjonen vil ikke fungere i det opprinnelige Macintosh-miljø. Se respektive brukerhåndbøker for detaljert support. Krav til å kjøre på et Macintosh-operativsystem kan finnes

- Vi anbefaler at vertdatamaskiner er oppdatert med de nyeste kritiske programutbedringene og serviceutgivelser fra Microsoft® Corporation.

- Nettverkets TCP/IP (Transmission Control Protocol/Internet Protocol) må være lastet og i gang.

- Administrative privilegier kreves for å installere enhetadministrasjonapplikasjonprogramvaren på klientmaskinen.

- Krever SNMP-aktiverte enheter og muligheten til å rute SNMP over nettverket. Det kreves ikke å aktivere SNMP på datamaskinen der Xerox® Device Management Applications vil bli installert eller på andre nettverkdatamaskiner.

- Microsoft®.NET Framework må være installert før applikasjonen installeres.

- Applikasjonen skal ikke installeres på en PC der andre SNMP-baserte applikasjoner eller andre Xerox®-utskriftadministrasjonverktøy er installert, da de kan forstyrre hverandres drift.

Databasekonfigurasjoner

- Applikasjonen installerer SQL Server Compact Edition (SQL CE)-databasemotor og -databasefiler som lagrer skriverdata- og applikasjoninnstillinger innenfor installasjonkatalogen. Det er ikke nødvendig med noen databaselisens for applikasjonen. Xerox® Device Agent støtter også eksisterende instanser av SQL Server, slik som beskrevet ovenfor.

Ikke-støttede konfigurasjoner

Dette avsnittet viser konfigurasjonene som ikke er støttet.

- Installasjon av applikasjonen på en datamaskin med en annen Xerox-enhetadministrasjonapplikasjon, slik som Xerox Device Manager.

- Innebygd Mac OS® operativsystemprogramvare (dvs. Xerox Device Agent kan kun kjøre på Apple Mac-plattformen når Parallels emulasjonprogramvare er installert.)

- Enhver versjon av UNIX®-operativsystemer, Linux®-operativsystemer, Windows®-systemer som kjører 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 som kjører terminaltjenester for applikasjoner og installasjon på Windows-systemer som kjører domenekontrollere.

Siden denne applikasjonen kun har blitt testet på VMware® Lab Manager/arbeidsstasjonmiljø, støttes ikke andre virtuelle miljøer støttet.

7. Xerox forretningsprosess og tjenester

Data mottatt fra Xerox® Office-baserte utskriftenheter, Xerox® Production-baserte utskriftenheter og Xerox Device Management Applications som en del av fjerntjenesteløsningen, brukes av Xerox forretningsprosesser som er opplistet nedenfor:

Tabell 5 fremstiller navn og beskrivelse av forretningsprosessen og tjenestene som støttes som en del av fjerntjenesteløsningen.

Navn på forretningsprosess	Beskrivelse
Automatiske måleravlesninger	Måleravlesningsdata brukes i faktureringsprosessen.
Automatisk forbruksvareforsyning / automatisk deleforsyning	Blekk sendes automatisk til kundene basert på forbruksvarens uttømmingstatus som mottas fra utskriftenhetene. Visse utskiftbare komponenter sendes automatisk til kunder ved behov for deres utskriftenheter. Disse alternativene er tilgjengelige for kunder som kun velger målte forsyningskontrakter.
Serviceevne (vedlikeholdassistent)	Fjern administrasjon av enheten gir detaljert feilinformasjon som kan vises av Xerox-servicepersonale, ved behov, for å ekspeditere klargjøringen for et besøk på stedet eller for å diagnostisere og løse problemer.
3.-nivå support (teknisk/utbedring)	Produktsupportpersonale kan utbedre vanskelige problemer når de får tilgang til detaljert teknologi og utbedringslogger.
Produktutvikling	Skriverytelse- og brukdata brukes til å identifisere produktforbedringer for fremtidige utgivelser.

Grunnleggende utskriftenhetdata aggregeres, overføres, beholdes og arkiveres innenfor et ISO-27001-sertifisert Xerox-datasenter og oppbevares i samsvar med oppbevaringsretningslinjer for Xerox-selskapdata.

Arbeidsprosessene og fremgangsmåtene som støtter og beskytter programvaresystemene for eksterne tjenester er basert på ITILs beste praksis og Xerox informasjonsikkerhet-policyer som er direkte i tråd med ISO 27002-standardene for styringssystem for informasjonsikkerhet i International Standards Organization. Kunder kan være sikre på at administrasjonen, beskyttelsen og oppbevaringen av enhetdata forstår de grunnleggende elementene i informasjonsikkerhet: konfidensialitet, integritet, tilgjengelighet, autentisering og ikke-avvisning.

8. Teknologidetaljer

Dette avsnittet gir ytterligere tekniske detaljer, som typisk kreves av informasjonteknologi (IT)-team og sikkerhetsutøvere som håndterer risikoer ved å oppnå garanti for sikre utviklingspraksiser. Slik forsikring gjør det mulig for dem å sertifisere våre utskriftenheter og enhetadministrasjonapplikasjoner for bruk innenfor kundens nettverkmiljø.

Programvaredesign

Vårt engasjement for Xerox-produktsikkerhet begynner tidlige i produktutviklingen der Xerox-utviklere følger en formell sikkerhetsutvikling-livssyklus som administrerer sikkerhetsproblemer gjennom identifisering, analyse, prioritering, koding og testing. Mange Xerox®-utskriftenheter er Common Criteria-sertifisert iht. ISO IEC 15408 eller er aktivt under sertifiseringsgjennomgang.

Driftevne

Xerox-fjerntjenester utfører følgende typer av operasjoner på et nettverk. Disse operasjonene avhenger av brukmetoden som er konfigurert.

Tabell 6.

Brukmetode	Brukt applikasjon	Dataflyt på nettverket	Driftevne pålagt et nettverk
Device Direct	Ingen	Intern	Xerox® Print Device gjør forsøk på å detektere en nettproksyserver (automatisk eller ledet til en spesifikk adresse)
		Intern	Xerox®-utskriftenheter kan programmeres til å generere forespørsler til en SMTP (Simple Mail Transport Protocol)-server for å sende varslingmeldinger på e-post til en definert mottakerliste
		Eksternt for nettverk	Xerox®-utskriftenhet går over selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Eksternt for nettverk	Xerox®-utskriftenhet autentiseres med sertifikatet til fjern Xerox-kommunikasjonserver før overføring av eventuelle dataattributter
		Eksternt for nettverk	Xerox®-utskriftenhet overfører automatisk utskriftenhetens attributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonservere ved et spesifisert tidspunkt daglig eller på kundens forespørsel.
		Eksternt for nettverk	Xerox®-utskriftenhet forespør automatisk Xerox®-kommunikasjonservere gjennom en kryptert kanal (HTTPS over port 443) ved et spesifisert tidspunkt hver dag for en liste over handlinger som skal utføres (dvs. sende faktureringsdata nå, legge til tjeneste osv.).
		Eksternt for nettverk	Enveis overføring på forespørsel av loggdata for Xerox® Print-enhetteknikk gjennom en kryptert kanal (HTTPS over port 443) til Xerox® kommunikasjonserver

Brukmetode	Brukt applikasjon	Dataflyt på nettverket	Driftevne pålagt et nettverk
Device Direct	Ingen	Utgående, initiert av dev til å trekke nyeste s/w	Enheten sender forespørsel til fjern programvareadministrasjonserver for å kontrollere med hensyn til programvare- / sikkerhetoppdateringer. Hvis kundemiljøet forbyr automatiske programvareoppdateringer, kan det fjernprogramvareadministrasjonalternativet velges bort kun uten avbrudd av standard fjerntjenester.
Enhetadministrasjonapplikasjoner	Centre Ware® Web	Intern	Hver app detekterer en nettproksyserver (automatisk eller ledet til en spesifikk adresse)
		Intern	Hver app henter ut utskriftenhetfunksjoner på tvers av flåten via SNMP
		Intern	Hver app henter ut utskriftenhetkonfigurasjon på tvers av flåten via SNMP
		Intern	Hver app henter ut utskriftenhetstatus på tvers av flåten via SNMP
		Intern	Hver app henter ut utskriftenhetforbruksvaredata på tvers av flåten via SNMP
		Intern	Hver app kan starte en utskriftenhet på nytt via SNMP eller via utskriftenhetens nettgrensesnitt
		Intern	Hver app kan sende inn en testside til en spesifikk utskriftenhet
		Intern	Hver app kan starte en utskriftenhet nettside
		Ekstern **(kun utgående)**	Hver app går over selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Ekstern **(kun utgående)**	Hver app autentiseres med sertifikatet til fjern Xerox-kommunikasjonserver før overføring av eventuelle dataattributter
		Ekstern **(kun utgående)**	Hver app overfører automatisk utskriftenhetens attributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonservere ved et spesifisert tidspunkt hver dag
		Ekstern **(kun utgående)**	Hver app forespør automatisk Xerox®-kommunikasjonservere gjennom en kryptert kanal (HTTPS over port 443) ved et spesifisert tidspunkt hver dag for en liste over handlinger som skal utføres
		Intern	Hver Xerox Device Agent-app detekterer en nettproksyserver (automatisk eller ledet til en spesifikk adresse)
		Intern	Hver XeroxDevice Agent-app henter ut utskriftenhetfunksjoner på tvers av flåten via SNMP
		Intern	Hver Xerox® Device Agent-app henter ut utskriftenhetkonfigurasjon på tvers av flåten via SNMP
		Intern	Hver Xerox Device Agent-app henter ut utskriftenhetstatus på tvers av flåten via SNMP
		Intern	Hver Xerox Device Agent-app henter ut utskriftenhetforbruksvaredata på tvers av flåten via SNMP

Brukmetode	Brukt applikasjon	Dataflyt på nettverket	Driftevne pålagt et nettverk
Enhetadministrasjonapplikasjoner	Xerox Device Agent Partner Edition for overvåkning av nettverk-tilkoblede utskrift-enheter	Intern	Hver Xerox Device Agent-app kan forespørre at enheten skriver ut en konfigurasjonrapport
		Intern	Hver Xerox Device Agent-app kan starte en utskriftenhets nettside
		Intern	Hver Xerox Device Agent-app kan oppgradere utskriftenhetens programvare via utskriftenhetinnlevering. (. DLM-fil over port 9100)
		Ekstern **(kun utgående)**	Hver Xerox Device Agent-app går over selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Ekstern **(kun utgående)**	Hver app autentiseres med sertifikatet til fjern Xerox-kommunikasjonserver før overføring av eventuelle dataattributter
		Ekstern **(kun utgående)**	Hver Xerox Device Agent-app overfører automatisk utskriftenhetens attributtdata gjennom en kryptert kanal (HTTPS over port 443) til Xerox®-kommunikasjonservere ved et spesifisert tidspunkt hver dag
		Ekstern **(kun utgående)**	Hver Xerox Device Agent-app forespørrer automatisk kommunikasjonservere gjennom en kryptert kanal (HTTPS over port 443) ved et spesifisert tidspunkt hver dag for en liste over handlinger som skal utføres.
	Xerox® Device Manager for overvåkning	Intern	Xerox Device Manager- / Xerox Device Agent-apper detekterer en nettproksyserver (automatisk eller ledet til en spesifikk adresse)
		Intern	Xerox Device Manager- / Xerox Device Agent-apper henter ut utskriftfunksjoner på tvers av flåten via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apper henter ut utskriftenhetkonfigurasjon på tvers av flåten via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apper henter ut utskriftenhetstatus på tvers av flåten via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apper henter ut utskriftenhetforbruksvaredata på tvers av flåten via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apper kan forespørre enheten om å skrive ut en konfigurasjonrapport
		Intern	Xerox Device Manager- / Xerox Device Agent-apper kan starte en utskriftenhets nettside
		Intern	Xerox Device Manager- / Xerox Device Agent-apper kan oppgradere utskriftenhetens programvare via utskriftenhetinnlevering.
		Intern	Xerox Device Manager-appen støtter SNMPv3-kommunikasjon m/utskriftenheter
		Intern	Xerox Device Manager-appen kan foreta endringer på utskriftenhetens konfigurasjon via SNMP og nettbrukergrensesnittet.

Brukmetode	Brukt applikasjon	Dataflyt på nettverket	Driftevne pålagt et nettverk
Enhetadministrasjonapplikasjoner	av nettverk-tilkoblede utskriftenheter	Intern	Xerox Device Manager-appen henter ut jobb-baserte regnskapslogger fra visse Xerox® MFP-er
		Intern	Xerox Device Manager-appen administrerer / implementerer utskriftkontrollretningslinjer
		Ekstern **(kun utgående)**	Xerox Device Manager- / Xerox Device Agent-apper går over selskapets brannmur for å få tilgang til Internett (HTTPS over port 443)
		Ekstern **(kun utgående)**	Hver app autentiseres med sertifikatet til fjern Xerox-kommunikasjonserver før overføring av eventuelle dataattributter
		Ekstern **(kun utgående)**	Xerox Device Manager- / Xerox Device Agent-apper overfører automatisk utskriftenhetdata til Xerox®-kommunikasjonservere gjennom en kryptert kanal (HTTPS over port 443) ved et spesifisert tidspunkt hver dag.
		Ekstern **(kun utgående)**	Xerox Device Manager- / Xerox Device Agent-apper forespør automatisk Xerox-kommunikasjonservere gjennom en kryptert kanal (HTTPS over port 443) ved et spesifisert tidspunkt hver dag for en liste over handlinger som skal utføres.
	Enhetadministrasjonapplikasjon	Ekstern, toveis	Xerox Device Manager kontakter Xerox Services Manager daglig og gjør det mluig for administratorer å fjernt endre innstillinger, slik at behovet for servicebesøk på stedet unngås.

9. Sikkerhetsegenskaper

SNMP (SIMPLE NETWORK MANAGEMENT PROTOCOL) FOR XEROX

SNMP (Simple Network Management Protocol) er det mest utbredt brukte nettverkadministrasjonverktøyet for kommunikasjon mellom nettverkadministrasjonsystemer og nettverktilkoblede skrivere. enhetadministrasjonapplikasjoner bruker SNMP i løpet av oppdagelseoperasjoner for å innhente detaljert utskriftenhetinformasjon. Xerox®-enhetadministrasjonapplikasjoner støtter SNMP v1/v2- og v3-protokoller. Se respektive Xerox®-enhetadministrasjonapplikasjon sertifiseringsguider for spesifikke detaljer.

SNMP v3-rammeverket støtter flere sikkerhetsmodeller, som kan finnes samtidig innenfor en SNMP-enhet. SNMPv3 inkluderer strammere sikkerhet ved å legge til kryptografisk sikkerhet til SNMPv2. I tillegg er SNMPv3 bakoverkompatibelt med tidligere versjon er og er utbredt i bruk på tvers av robuste nettverk.

Xerox-enhetadministrasjonapplikasjoner (Centre Ware® Web / Xerox Device Manager, Xerox Device Agent) kan kommunisere med enhetplattformer som er kompatible med Federal Information Processing Standard FIPS 140-2 i sine implementeringer av SNMPv3.

Xerox-enhetadministrasjonapplikasjonene bruker ikke Windows SNMP-tjenesten eller Windows SNMP Trap-tjenesten. Hvis tidligere installert, **må** disse tjenestene deaktiveres på enhver personlig datamaskin (PC) eller server der Xerox-enhetadministrasjonapplikasjonen er installert.

Xerox-enhetadministrasjonapplikasjonene bruker en Xerox-utviklet SNMP-agent som:

- Inneholder en spesiell koding-/avkodingsmekanisme
- Er fullstendig .NET-administrert
- Bruker .NET-drifttidsutføring-element – dette gir forbedret sikkerhet for å forhindre angrep mot programvaresårbarheter som ugyldige pekermanipuleringer, bufferoverkjøringer og bundet kontroll.

Xerox-enhetadministrasjonapplikasjonene bruker sikkerhetsfunksjonene som er tilgjengelige fra Windows-operativsystemet (OS), inkludert:

- Brukerautentisering og -autorisasjon
- Tjenestekonfigurasjon og -administrasjon
- Grupperetningslinjebruk og -administrasjon

Windows Internet Connection Firewall (ICF), inkludert:

- Innstillinger for sikker innlogging

- ICMP-innstillinger

Xerox-enhetadministrasjonapplikasjoner: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE-applikasjon Microsoft® SQL Server og **Xerox Device Manager** bruk Microsoft® SQL Server.

Xerox-enhetadministrasjonapplikasjoner kan konfigureres for å utnytte ytterligere Microsoft®-sikkerhetsfunksjoner, slik at de inkluderer, der det er aktuelt:

- Aktivere brukerkontoregistrering
- Kryptering av DNS (Domain Name System)
- Begrense brukerkontoprivilegier til å få tilgang til databasen (dvs. databaseeierrettigheter)
- Implementering av brukerdefinerte portnumre

En Xerox-registreringsnøkkel og en gyldig Xerox-konto er nødvendig for å overføre data til fjern-Xerox-kommunikasjonservere.

Xerox-enhetadministrasjonapplikasjonenes eksterne kommunikasjon kan påvirkes av Windows Internet Connection Firewall (ICF). (Vi **anbefaler** at kunder hvitelister Xerox URL på kundens brannmur (*.support.xerox.com) og spesifiserer IP-adressen som kan få tilgang til URL.)

Xerox-enhetadministrasjonapplikasjoner kjører som en bakgrunnprosess ved bruk av lokale kontoopplysninger for å automatisk forespørre nettverkutskriftenheter via SNMP og periodisk overføre utskriftenhetattributter tilbake til Xerox-kommunikasjonservere.

Tilgang til Xerox Device Manager-applikasjonens brukergrensesnitt (UI) og funksjoner kontrolleres via følgende rollebaserte privilegier:

- Centre Ware® Web-administratorer, Centre Ware® Web Power-brukere, Centre Ware® Web SQL-brukere, Centre Ware® Web-kundeadministratorer og Centre Ware® Web-kundegrupper.
- Brukernavn og passord for applikasjonene går ikke over nettverket; tilgangstokener er brukt i stedet (av Windows® OS-design).
- Xerox Device Manager-applikasjonen gir utskriftinnsendingskontrollbasert sikkerhet ved å begrense jobber basert på retningslinjer for fargebruk, dokumenttype, jobbkostnad, tid på dagen, brukergruppetilgangkontroll, dupleksretningslinjer, jobbinntrykk tillatt og utskriftkvoter.

Merk: Bruk av SNMP av enhver Xerox® fjernserviceapplikasjon utgjør ingen sikkerhetsrisiko for en klients IT-miljø, fordi all SNMP-basert trafikk som er generert eller forbrukt av disse applikasjonene, forekommer innenfor klientens Intranet, bak brannmuren. Windows SNMP-tjeneste og Windows SNMP Trap-tjeneste er ikke aktivert innenfor Windows OS som standard.

Selskapsikkerhetmodus

Den ***planlagte*** synkroniseringen av Xerox Device Agent-applikasjonen til den sikre kommunikasjonserveren er stilt på *daglig*, som standard. Merk at tidspunktet på dagen kan stilles inn på et valgt klokkeslett.

Det finnes to moduser for selskapsikkerhet: **Normal** og **Avsperret.**

Hvis stilt på **Normal**-modus, kontakter enhetadministrasjonapplikasjonen Xerox Services Manager daglig. Innstillinger kan endres uten behov for besøk på stedet, selv når forespørselplaner er slått av. ***(Anbefalt modus***).

I **Låst-modus**, unntatt skriverrelatert datasynkronisering er det ingen kommunikasjon med kommunikasjonserverne, og innstillingene må endres på stedet. I tillegg er Xerox Device Agent-maskins og -skrivers IP-adresser ikke rapportert til kommunikasjonserveren. Denne modusen begrenser alle andre fjerntjenestefordeler til å inkludere automatisk fakturering og forsyninger, samt diagnostiske data som brukes til teknisk support.

Merk: Hvis en Xerox Device Agent-versjon ikke inneholder modusfanen for selskapsikkerhet, drives den i Normal-modus.

10. Nettverkpåvirkning

Selskapnettverkretningslinjer vil typisk aktivere eller deaktivere spesifikke nettverkporter på rutere og/eller servere. De feste IT-avdelinger er bekymret for portene som brukes av applikasjonen for utgående trafikk. Deaktivering av spesifikke porter kan påvirke applikasjonens funksjonalitet. Se tabellen nedenfor for spesifikke porter som brukes av applikasjonens prosesser. Hvis applikasjonen kreves for å skanne over flere nettverksegmenter eller subnett, må rutere tillate protokollene tilknyttet disse portnumrene.

Protokoller, porter og andre relaterte teknologier

Tabell 7 identifiserer protokollene, portene og teknologiene som brukes innenfor Xerox® Remote Services:

Portnummer	Protokoll	Beskrivelse av bruk	Dataflyt på nettverket
Avhengig av øvre lagprotokoller	**Internettprotokoll (IP)**	**Underliggende transport for all datakommunikasjon**	**Intern + ekstern (kun utgående)**
IR	Internet Control Message-protokoll (ICMP)	Utskriftenhetoppdagelse + feilsøking	Intern
25	Simple Mail Transport Protocol (SMTP)	Utskriftenhet + fjernvarslinger om proksyapp-e-postmeldinger	Intern
53	DNS (Domain Name System)	Brukes for DNS-baserte utskriftenhet oppdagelseoperasjoner	Intern
80	Hyper Text Transport Protocol (HTTP)	Utskriftenhet nettsideforespørsler + enhetadministrasjonapplikasjon, nettsideforespørsler	Intern
135	Remote Procedure Call (RPC)	utskriftenhetoppdagelse	Intern
161	SNMP (Simple Network Management Protocol) (SNMP v1 / v2C / v3)	Industriprotokoller som brukes til å oppdage nettverktilkoblede utskriftenheter + Innhente status, tellere og forsyningsdata + Hente inn og bruke utskriftenhetkonfigurasjon. Standard miljønavn = "offentlig" (GET), "privat" (SET)	Intern

Portnummer	Protokoll	Beskrivelse av bruk	Dataflyt på nettverket
443	Hyper Text Transport Protocol Secure (HTTPS)	Utskriftenhet sikre nettsideforespørsler (hvis konfigurert) + fjern proksyapp sikre nettsideforespørsler (hvis konfigurert) + Utskriftenhetdata overføring tilbake til Xerox®-kommunikasjonservere + utskriftkontrollkommunikasjon tilbake til Xerox® Device Manager	Intern + ekstern (kun utgående)
515, 9100, 2000, 2105	TCP/IP LPR og Raw Port utskriftjobbinnlevering	Utskriftenhet, programvareoppgradering + Skriv ut testsidediagnostikk	Intern

11. Beste praksis for sikkerhet

- Hold alltid utskriftenheter oppdatert med nyeste fastvare/programvare. Xerox overvåker sårbarheter og gir proaktivt kunder sikkerhetsutbedringer og -oppdateringer, ved behov.
- Deaktiver ubrukte porter og protokoller på utskriftenheter der mulig. Dette er typisk utført på nettbrukergrensesnittet (UI) for kontorklasseutskriftenheter og lokalt brukergrensesnitt (UI) for produksjonklasseutskriftenheter.
- Utnytt brukertilgangkontrollrelaterte funksjoner på utskriftenheter, hvis tilgjengelig. Dette er typisk utført på nettbrukergrensesnittet (UI) for kontorklasseutskriftenheter og lokalt brukergrensesnitt (UI) for produksjonklasseutskriftenheter.
- Utnytt sikre protokoller når det er mulig. Dette er typisk utført på nettbrukergrensesnittet (UI) for kontorbaserte utskriftenheter og lokalt brukergrensesnitt (UI) for produksjonbaserte utskriftenheter.
- Aktiver sikkerhetsfunksjoner som er integrert innenfor enheten (dvs. bildeoverskriving, skanningsdatakryptering, utskriftstrømkryptering, diskkryptering, sikker utskrift, kryptert .pdf, CAC/PIV tilgangautentisering.)

For å finne ytterligere informasjon vedrørende fjerntjenester hos Xerox, besøk Xerox.com/RemoteServices.

For ytterligere og spesifikk informasjon vedrørende sikkerhetsmekanismer og -egenskaper innenfor serien av Xerox-enhetadministrasjonapplikasjoner, se deres respektive veiledninger:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Enten det er enhet- eller innholdsikkerhet, er Xerox ledende med proaktiv sikkerhet for dagens tiltakende trusler. Besøk www.xerox.com/security for å få tilgang til en full bredde av sikkerhetsinformasjon, oppdateringer, nyhetsmeldinger, produktdokumentasjon, utbedringer og mer.