Xerox® Remote Services

Hvidbog om sikkerhed

Version 2.0

Globale Remote Services

Xerox® Technology Information Management

Januar 2017

BR19369

Dette dokument ændres med jævne mellemrum. Ændringer, tekniske unøjagtigheder og typografiske fejl korrigeres i efterfølgende udgaver.

IS 614672/IS 514590

Dokumentversion: 2.0 (januar 2017).

Indholdsfortegnelse

Generelt formål og målgruppe

Formålet med dette dokument er at fungere som en vejledning i udrulning af Xerox® Remote Services til netværkstilsluttede printere af typen Xerox og andre i kundens miljø. Det er hensigten at give sikkerhedsrelaterede oplysninger og indsigt i de omfattende sikkerhedsforanstaltninger, der er implementeret i Xerox® Remote Services.

Målgruppen for dette dokument omfatter tekniske leverandører, IT-netværksadministratorer og IT-sikkerhedspersonale, der interesserer sig for funktionerne i Remote Services og for sikkerhedsimplementeringen af disse.

Vi anbefaler, at dokumentet læses i sin helhed for at verificere brugen af Xerox®-produkter og -tjenester i netværksmiljøet hos en kunde.

Remote Services

Oplysninger er et vigtigt aktiv, og sikkerhed er afgørende for alle organisatoriske aktiver, herunder netværkstilsluttede multifunktionsprintere (MFP'ere). Med nutidens "alt-i-én"-løsninger giver det at skulle styre en flåde af multifunktionsprintere og samtidig sikre et acceptabelt sikkerhedsniveau, en række unikke udfordringer, der ofte overses. Xerox® forstår denne kompleksitet og reagerer på kundernes sikkerhedsbehov. Xerox®-produkter, Xerox®-systemer og Xerox® Remote Services-løsninger er udviklet til sikker integration med kundernes eksisterende arbejdsgange og anvender samtidigt de sidste nye teknologier.

Hvidbogen om sikkerhed i Xerox® Remote Services har til formål at hjælpe kunden med at forstå og anvende den korrekte og sikre Remote Services-løsning, der er kompatibel med kundens netværksinfrastruktur. Opbygningen af kundens netværk er afgørende for, om det er nødvendigt at ændre internetfirewall, web-proxy-servere eller anden sikkerhedsrelateret netværksinfrastruktur. Valget af Xerox® Remote Services-løsning, enhed og kontroller afhænger af kundens politikker for informationssikkerhed (IS) og er afgørende for, hvilken driftsform der bruges.

Xerox® Remote Services-funktionen understøttes af visse modeller. Denne funktion gør det muligt at udføre fjernservice og -support på printere ved hjælp af printenhedens attributdata, som omfatter: ***Printenhedens identitet, egenskaber, status, niveau af forbrugsstoffer, brugsdata og detaljerede diagnostikdata***. Printenhedens attributdata sendes direkte fra printenheden (Device Direct) i kundens netværksmiljø via en hosted applikation (administrationsapplikation) eller via en kombination af begge metoder med den sikre Xerox® Remote Services-kommunikationssti. Både Xerox®-enheder og Xerox®-administrationsapplikationer har et certifikat, der skal godkendes af Xerox® Communications Servers, før overførsel af printenhedernes attributter kan finde sted. Xerox® Remote Services-transaktioner kommer altid fra kundens miljø og sendes udelukkende på baggrund af kundens godkendelser.

Xerox® Communications Servers er baseret i USA og overholder de strenge sikkerhedskrav for informationssikkerhedsstyring. Xerox® Datacenters og Xerox® Remote Services-applikationen er omfattet af den årlige SSAE (Statement on Standards for Attestation) nr. 16, kravene i SOX (Sarbanes-Oxley Act) og er ISO 27001:2013-certificeret.

Ingen af kundens billeder fra print, fax, scanning og kopiering eller følsomme oplysninger overføres som standard til Xerox® Communication Servers.

Kundens kontrol

Xerox® Device Management-applikationer kan vise eksporterede logs med printenhedens attributdata til revision og verifikationsformål før kryptering og overførsel til eksterne Xerox® Communication Servers. Se brugervejledningen til Xerox® Device Management-applikationen for specifikke oplysninger.

Nogle små til mellemstore kontorprintenheder er udstyret med en funktion, der gør det muligt for kunderne at downloade og gennemse printenhedens attributdata før kryptering og overførsel til de eksterne Xerox® Communication Servers via metoden til Device Direct-aktivering. Hvis du vil kontrollere, om en bestemt printenhed har denne funktion, skal du gå til printenhedens Centreware Internet Services-side; fanen Status, linket Smart eSolutions (eller Remote Services) og under fanen Maintenance Assistant (vedligeholdelsesassistent).

Xerox® Remote Services kan skræddersys til at håndtere kundernes IS-politikker, der væsentligt begrænser eller indskrænker bestemte typer af printenhedsattributter, som kan overføres uden for netværket (f.eks. netværksadresserelaterede attributter). Værktøjerne i Xerox® Device Management-applikationen kan bruges til at deaktivere udvalgte felter fra overførslen.

Kunderne har også mulighed for at benytte sig af en *Undtagelsesanmodning* under kontraktforhandlinger for at **"fravælge"** Remote Services-løsningen. Denne mulighed forhindrer al Remote Services-kommunikation og fjernsupport til printenhederne i den pågældende konto.

Hvis kunderne har behov for at løse eskalerede fjernsupportaktiviteter, kan de aktivere Remote Access-funktionen efter behov for at modtage printenhedens softwareudgivelser, sikkerhedsrettelser og fjerndiagnoser, reparation eller ændring af printenhedens konfigurationer og dermed afhjælpe eventuelle diagnosticerede fejl. Remote Access giver ikke Xerox® mulighed for at se eller downloade kundernes dokumenter, data eller andre oplysninger, der findes på eller sendes via printenheden eller kundens informationssystemer. Der er dog en undtagelse for dette, som opstår, når en kunde arbejder sammen med Xerox-supportmedarbejdere på at løse et vanskeligt problem, og der er behov for flere oplysninger for at kunne udføre en tilstrækkelig fejlfinding af problemet. I så fald kan kunden vælge at give Xerox tilladelse til at få adgang til de logs, der ligger lokalt på enheden, og som indeholder følsomme data.

Derfor opfordres virksomhedens IT-teams og sikkerhedsmedarbejdere til at læse hele dette dokument for at forstå de forskellige funktioner, krav og metoder i Xerox® Remote Services, og hvordan de understøtter overholdelse af virksomhedens IS-politikker.

Du kan finde flere sikkerhedsressourcer om databeskyttelse på Xerox®-produkter, branchepartnere og certificeringer på http://www.xerox.com/security.

Udrulningsmodeller

Kunderne kan vælge mellem følgende lige sikre Xerox® Remote Services-udrulningsmodeller:

- **Device Direct-modellen** – Device Direct gør det muligt for printenheder at kommunikere direkte med eksterne Xerox® Communication Servers via internettet gennem kundens firewall.

- **Device Management-applikationsmodellen** – En Xerox® Device Management-applikation (kaldet Device Manager) kan udrulles på kundens netværk for at indsamle et undersæt af dataattributter fra printenheder. Flere attributter til printenheden indsamles og overføres derefter sikkert til de eksterne Xerox® Communication Servers.

- **Kombinations-modellen** – Implementering af både Device Direct-modellen og Device Management-applikationsmodellen.

Alle udrulningsmodeller til Xerox® Remote Services udnytter branchestandardens webbaserede protokoller og porte til at etablere en sikker, krypteret kanal til overførsel af printenhedsattributter eksternt til Xerox® Communication Servers, der befinder sig på sikre Xerox®-datacentre.

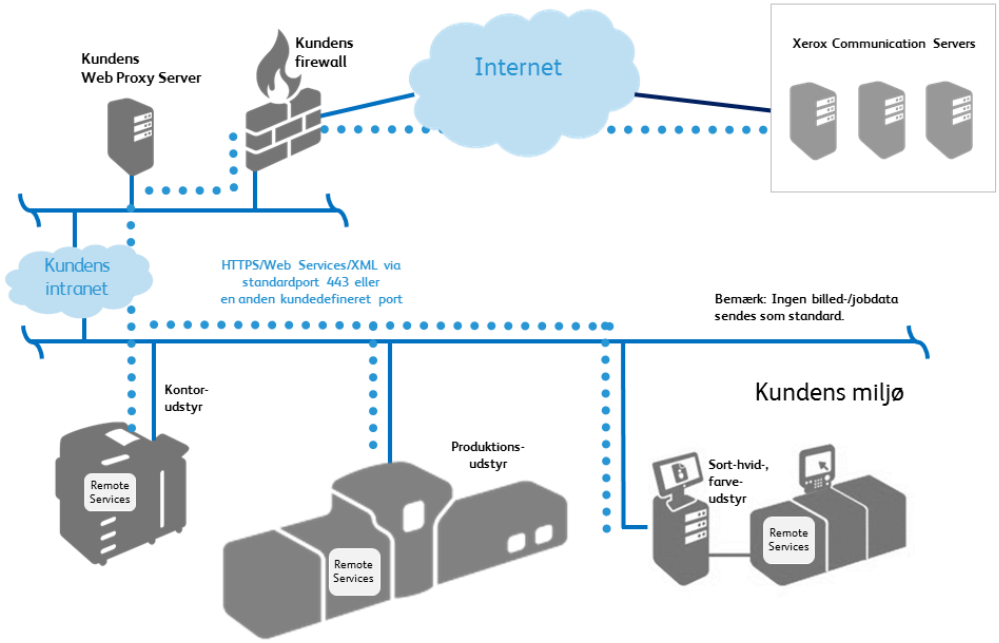
Den udrulningsmodel, der vælges, afhænger af kundernes IS-politikker og regler for håndtering af overførsel af printenhedens attributter og typen af printserviceløsning og de Xerox®-enheder, der er købt (basis eller Managed Print Services).

Device Direct-udrulningsmodel

Remote Services-modulet, der er integreret i Xerox®-enheder, benytter en 1.2 TLS-forbindelse (Transport Layer Security) via standardporten 443 til at kommunikere med de eksterne Xerox® Communication Servers.

- Printenheder i kundens miljø starter al kommunikation direkte med de eksterne Xerox® Communications Servers. Aktivering af kommunikationen kræver standard-firewallkonfigurationer på stedet.
- Der skal benyttes en gyldig URL til de eksterne Xerox® Communications Servers.
- Xerox® Communications Servers er placeret bag en sikker firewall, og der er ikke adgang til dem fra internettet.

Figur 1



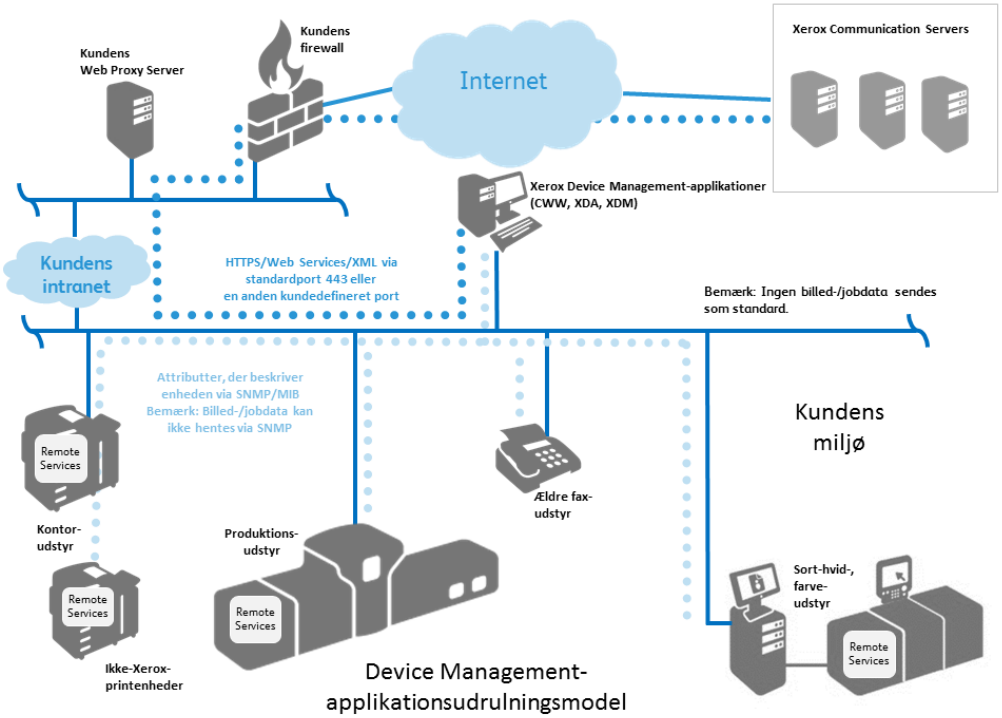
Device Direct-udrulningsmodel

Device Management-applikationsudrulningsmodel

Device Management-applikationerne (dvs. **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition og Xerox® Device Manager)** benytter også en sikker krypteret forbindelse af typen TLS 1.2 (Transport Layer Security) via standardport 443 til at kommunikere med de eksterne Xerox® Communication Servers. Andre funktioner, der benyttes for at forbedre sikkerheden på denne kanal og som etableres under installationen af Device Management-applikationerne, omfatter:

- Device Management-applikationen i kundens miljø starter al kommunikation med de eksterne Xerox® Communications Servers. Aktivering af kommunikationen kræver standard-firewallkonfigurationer på stedet.
- Der skal benyttes en gyldig URL til de eksterne Xerox® Communications Servers.
- Xerox® Communications Servers er placeret bag en sikker firewall, og der er ikke adgang til dem fra internettet.
- Der skal enten bruges et gyldigt konto-id eller et sted-id samt en Xerox® Communications Server-registreringsnøgle for at få adgang til nogle af tjenesterne på Xerox® Communication Servers.
- Device Management-applikationen kræver registrering på de eksterne Xerox® Communications Servers med de korrekte brugeroplysninger til certifikatgodkendelse.
- De eksterne Xerox® Communications Servers validerer de angivne brugeroplysninger og accepterer anmodningerne.
- Device Management-applikationen godkender de eksterne Xerox® Communications Servers og aktiverer tjenesten.

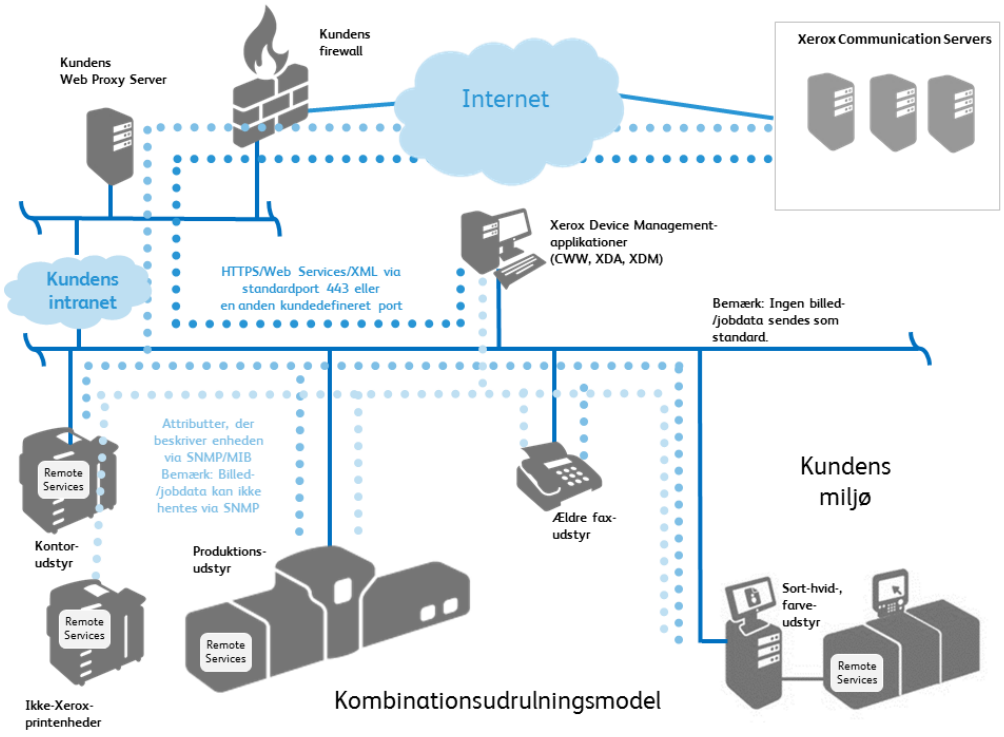
Figur 2



Kombinationsudrulningsmodel

Kombinationsudrulningen bruges, når en kunde køber flere typer Xerox-vedligeholdelsesaftaler til sine printenheder. Første gang en Xerox®-printenhed installeres på et netværk, forsøger Xerox® Remote Services som standard at etablere en direkte forbindelse mellem printenheden og Xerox® Communication Servers.

Figur 3



Dataoverførsel og data

Datakilder

Printenhedens dataattributter indsamles til Xerox® Remote Services fra følgende kilder:

- Xerox®-netværksprintere til kontoret
- Netværksprintere fra andre end Xerox®
- Xerox®-produktionsprintere
- Xerox® Device Management-applikationer

Xerox®-kontorenheder

Xerox®-printenheder i kontorklassen overfører enhedsdataattributter i XML-format (eXtensible Markup Language) som en komprimeret .zip-fil. Hver fil overføres derefter via en krypteret kanal til de eksterne Xerox® Communication Servers.

Tabel 1 identificerer de enhedsdataattributter, der kan overføres og deres beskrivelse.

Dataattributter	Beskrivelse
Printenhedens identitet	Omfatter model, firmwareniveau, modulets serienumre og installationsdato.
Printenhedens netværksadresse	Omfatter MAC-adresser (Media Access Control) og subnet-adresser.
Printenhedens egenskaber	Omfatter detaljeret hardwarekomponent-konfiguration, detaljeret softwaremodul-konfiguration, understøttede funktioner/services, strømsparetilstande osv.
Printenhedens status	Omfatter overordnet status, detaljerede advarsler, historik for de seneste 40 fejl, data om blokeringer osv.
Printenhedens tællere	Omfatter faktureringsmålere, printrelaterede tællere, kopirelaterede tællere, faxrelaterede tæller, storjobs-relaterede tællere, scanning-til-destination-relaterede tællere, anvendelsesstatistikker osv.
Printenhedens forbrugsvarer	Omfatter forbrugsvarens navn, type (f.eks. billeder, finishing, papirmedie), niveau, kapacitet, status, størrelse osv.
Print detaljeret brug af maskine	Omfatter detaljerede printrelaterede tællere, tænd/sluk-tilstande, detaljerede CRU-udskiftningsmængder (Customer Replaceable Units), detaljerede data for CRU-fejl og fordeling, anvendelse af integreret OCR-funktion (Optical Character Recognition), fordeling af kørselslængde for print, fordeling af anvendelse af papirbakker, installeret medie, fordeling af medietyper, fordeling af dokumentlængde, antal sæt, HFSI-data, NVM-data, fordeling, optælling af markerede pixels, gennemsnitlig områdedækning pr. farve, fejl/blokeringer, detaljerede scanningsrelaterede tællere.

Dataattributter	Beskrivelse
Teknik/fejlfinding	Inkluderer detaljerede fejlfindingsoplysninger, der kan omfatte data ud over ovennævnte datasæt. Disse data kan omfatte PII, f.eks. brugernavne, e-mailadresser og jobdata. Dataene sendes med udtrykkelig tilladelse fra kunden og er kun beregnet til eskaleret support.

Bemærk: Filen og indholdet af de data, der identificeres, varierer afhængigt af produktmodellen.

Xerox®-produktionsenheder

Xerox®-printenheder i produktionsklassen overfører enhedsdataattributter i XML-format (eXtensible Markup Language) som en komprimeret .zip-fil. Hver fil overføres derefter via en krypteret kanal til de eksterne Xerox® Communication Services.

Tabel 2 identificerer de enhedsdataattributter og deres beskrivelse, der kan overføres.

Dataattributter	Detaljeret beskrivelse af dataattributter
Printenhedens identitet	Omfatter model, modul-firmwareniveauer, modul-serienumre, modul-installationsdatoer, kundens kontaktoplysninger, licensdata og placering, hvis muligt.
Printenhedens netværksadresse	Omfatter MAC-adresser (Media Access Control) og subnet-adresser.
Printenhedens egenskaber	Omfatter detaljeret hardwarekomponent-konfiguration, detaljeret softwaremodul-konfiguration, understøttede funktioner/services osv.
Printenhedens status	Omfatter aktive statusser, optælling af fejlhistorik, DFE hændelseslog, historik for dataoverførsel
Printenhedens tællere	Omfatter faktureringsmålere, printrelaterede tællere, kopirelaterede tællere, storjobs-relaterede tællere, produktionsspecifikke tællere, scan-til-destination-relaterede tællere på low-end produktionsmodeller osv.
Printenhedens forbrugsvarer	Omfatter producent, model, serienummer, navn, type, niveau, kapacitet, status, levetidstællere osv.
Print detaljeret brug af maskine	Omfatter HFSI data, NVM data, udskiftning af dele, DFE logs, detaljerede diagnostik-data, fejlløsning.
Teknik/fejlfinding	Omfatter ikke-strukturerede, detaljerede fejlfindingsrelaterede data, der kun er beregnet til niveau 3 support.
Kunde job-relateret	Xerox®-produktionsprintprodukter gør det muligt at genskabe jobrelaterede data som støtte for eskalerede supportscenarier via krypteret PostScript til Xerox. Det er kunden, der kontrollerer, om denne funktion skal aktiveres. Hvis kunden vælger at overføre jobrelaterede data (dvs. krypteret PostScript) tilbage til Xerox, håndteres dataene i overensstemmelse med Xerox' IS-politikker og standarder.

Der er tale om eskalerede supportscenarier, når detaljerede fejlfindingsoplysninger indeholder dataattributter, der ligger uden for datasættene i tabel 1-3. Dataene sendes med udtrykkelig tilladelse fra kunden og håndteres i henhold til Xerox' IS-politikker og standarder.

Bemærk: Filen og indholdet af de data, der identificeres, varierer afhængigt af produktmodellen.

Xerox® Device Management-applikationer

Xerox® Device Management-applikationer (dvs. Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**) og Xerox® Device Manager (**XDM**) overfører printattributdata i XML-format (eXtensible Markup Language) som en komprimeret .zip-fil. Filen krypteres derefter og overføres via krypterede kanaler til de eksterne Xerox® Communications Servers.

Tabel 3 identificerer de enhedsdataattributter og deres beskrivelse, der kan sendes via Xerox® Device Management-applikationen.

Dataattributter	Detaljeret beskrivelse af dataattributter
Printenhedens identitet	Omfatter producent, model, beskrivelse, firmware-niveau, serienummer, aktiv-tags, systemnavn, kontakt, placering, administrationstilstand for arbejdsstation (computer), faxnummer og kønavn.
Printenhedens netværksadresse	Omfatter MAC-adresse, IP-adresse, DNS-navn, subnet-maske, IP-standardgateway, sidst kendte IP-adresse, ændret IP-adresse, tidszone, IPX-adresse, IPX eksternt netværksnummer, IPX-printserver.
Printenhedens egenskaber	Omfatter installerede komponenter, komponentbeskrivelser, understøttede egenskaber/services, printhastighed, understøttede farver, finishing muligheder, duplex support, mærkningsteknologi, harddisk, RAM, understøttede sprog, brugerdefinerede egenskaber.
Printenhedens status	Omfatter overordnet status, detaljerede alarmer, meddelelser fra lokal konsol, komponentstatus, status for hentnings-relaterede data, registreringsdato, registreringsmetode/-type, enhedens oppetid, understøttede/aktiverede traps.
Printenhedens tællere	Omfatter faktureringsmålere, printrelaterede tællere, kopirelaterede tællere, faxrelaterede tæller, storjob-relaterede tællere, scanningsrelaterede tællere, anvendelsesstatistikker og målvolumen.
Printenhedens forbrugsvarer	Omfatter forbrugsvarens navn, type (f.eks. billeder, finishing, papirmedie), niveau, kapacitet, status, størrelse osv.
Printenhedens detaljerede benyttelse	Brugerbaserede jobsporingsdata inklusive jobkarakteristika (id, dokumentnavn, ejer, dokumenttype, jobtype, farve, duplex, krævet medie, størrelse, sider, sæt, fejl), destination (printenhed, model, DNS-navn, IP-adresse, MAC-adresse, serienummer), resultater af jobudskrivning (indsendelsestid, jobudskrivningstid, sider udskrevet, farve/sort-hvid sider udskrevet, anvendt farvetilstand, N-up), regnskabsdata (tilbageførselskode, tilbageførselspris, regnskabskilde), printjobbets kilde (arbejdsstation, printserver-navn/MAC-adresse, kønavn, port, brugernavn, bruger-id), Xerox-administrationsdata (sendt til Xerox® Services Manager).
Device Management-id	Omfatter oplysninger om applikationsværts-pc'en, f.eks. DNS-navn, IP-adresse, OS-navn, OS-type, pc'ens CPU, RAM-størrelse (ledig/anvendt), harddiskstørrelse (ledig/anvendt), stednavn, appversion, applicensens udløbsdato, .Net-version, tidszone, registreringsversion, hoveddatabasestørrelse, registreringsdatabasens størrelse, antal printere/ in scope/out of scope, kørende kritiske tjenester.

Dataattributter	Detaljeret beskrivelse af dataattributter
Virksomhedens sikkerhedstilstand i Device Manager	**Normal tilstand** = Xerox® Device Agent kontakter dagligt Xerox® Services Manager. Indstillingerne kan fjernredigeres uden behov for et besøg på stedet, selvom pollingplaner er slået fra. **Spærret tilstand** = Ud over printerrelateret datasynkronisering er der ingen kommunikation med Xerox® Services Manager, og indstillingerne skal ændres på stedet. Xerox® Device Agent-maskinen og printerens IP-adresser rapporteres til Xerox® Services Manager.
Device Management-printkontrolpolitik	Omfatter navn på slutbrugerens pc, anvendt printserver, anvendt printkø, tidsstempel for brud, dokumentnavn, slutbrugers brugernavn, job-duplex, jobfarve, samlet antal kopier af job, jobpris, handling foretaget, slutbruger notificeret, meddelelse vist, printpolitikkens navn, printpolitikregel.

Fjernadministration af printenheder

Xerox®-supportmedarbejdere kan udføre følgende handlinger via Xerox® Device Management-applikationen. Disse handlinger udføres, som støtte for løsning af unormale tilstande, såfremt brugeren tillader det. Handlingerne er afgrænset i **tabel 4** nedenfor.

Data	Beskrivelse
Handlinger, der skal udføres på printenheder	• **Hent enhedens status** = hent seneste status fra printenhed • **Genstart enhed** = start en sluk/tænd-sekvens på printenheden • **Opgrader enhed** = installer ny software/firmware på printenhed (.DLM via port 9100) • **Fejlfind enhed** = ping enhed + hent seneste status fra printenhed • **Udskriv testside** = send et testjob til en printenhed for at validere printstien (generer en konfigurationsrapport) • **Start administration af enhed** = start regelmæssige dataoverførsler fra printenhed til Xerox® Communication Servers **Bemærk:** Hver handling kan deaktiveres fra brug efter behov i administrationskonfigurationsdelen i Xerox® Device Management-applikationer, der understøtter denne funktion.
Handlinger, der skal udføres på printenheder	• **Genstart enhed** = start en sluk/tænd-sekvens på printenheden • **Udskriv testside** = send et testjob til en printenhed for at validere printstien (generer en konfigurationsrapport)
Handlinger, der kan udføres i Device Management-applikationer	Indstillinger i hver enkelt Device Management-applikation, der kan styres, omfatter registreringshandling, dataeksportfrekvens, SNMP-kommunikationsrelaterede indstillinger (forsøg igen, timeout, community-navne), advarselsprofiler og frekvens for automatisk opdatering af Device Management-applikationens software.

Systemkrav for Device Management-applikationer

Minimumskravene varierer lidt afhængigt af produkterne. Se brugervejledningen, guiden om sikkerhedsevaluering og/eller certificeringsguiden for grundkrav, der er specifikke for den pågældende Device Management-applikation. Du kan finde flere oplysninger på: http://www.support.xerox.com/support/enus.html

Under installationen inkluderes der en .readme-fil, som indeholder yderligere og specifikke systemkrav for den Device Management-applikation, der installeres.

- Vi anbefaler, at værtscomputere kører et understøttet operativsystem fra Microsoft® Corporation. Men Xerox® Device Management-applikationer kan køre i et Macintosh OS-miljø, hvis der bruges emuleringssoftware fra Parallels Desktop. (Du kan ikke køre Xerox® Device Management-applikationen i et normalt Macintosh-miljø). Se brugervejledningen til Xerox® Device Management-applikationen for yderligere oplysninger.
- Vi anbefaler, at værtscomputere opdateres med de nyeste vigtige programrettelser og serviceudgivelser fra Microsoft® Corporation.
- Netværkets TCP/IP skal være indlæst og fungere.
- Der kræves en internetforbindelse.
- Der kræves administratorrettigheder for at installere Device Management-applikationens software på klientmaskiner.
- Kræver SNMP-aktiverede enheder og mulighed for at distribuere SNMP via netværket. Det er ikke et krav at aktivere SNMP på den computer, hvor Xerox® Device Management-applikationerne installeres eller på andre netværkscomputere.
- Du skal installere Microsoft®.NET Framework 4.6 (fuld version), før du installerer applikationen.
- Applikationen må ikke installeres på en pc, hvor andre SNMP-baserede applikationer eller andre Xerox® Device Management-værktøjer er installeret, da de kan forstyrre hinanden.

Ikke-understøttede konfigurationer

- Installation af applikationen på en computer med en anden Xerox® Device Management-applikation, f.eks. Xerox® Device Manager.
- Et Unix®- eller Linux®-operativsystem.
- Microsoft®-operativsystemer som er udfaset, f.eks. Windows NT® 4.0, Windows® Media Center, Windows® XP og Windows® Server 2000 og 2003.
- Andre virtuelle miljøer end VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Denne applikation fungerer muligvis i andre virtuelle miljøer, men disse miljøer er ikke blevet testet.

Xerox®-forretningsproces og tjenester

De data, der modtages af Xerox® Communication Servers fra Xerox® kontorbaserede printenheder, Xerox® produktionsbaserede printenheder og Xerox® Device Management-applikationer benyttes af følgende Xerox-forretningsprocesser:

Forretningsprocessens navn	Beskrivelse
Automatiske måleraflæsninger	Der dannes automatisk en faktura ud fra målerdata, der modtages fra printenheder.
Automatisk opfyldning af forbrugsvarer/Automatisk genopfyldning af reservedele	Der sendes automatisk toner til kunderne, når der modtages en tømningsstatus fra printenheder. Udskiftelige komponenter sendes automatisk til kunderne, når de har brug for dem til deres printenheder. Disse muligheder er kun tilgængelige for kunder, der kun vælger målerbaserede forsyningsaftaler.
Anvendelighed (vedligeholdelsesassistent)	Xerox-servicemedarbejdere kan få vist detaljerede fejloplysninger, når det er nødvendigt for at fremskynde forberedelse af et servicebesøg på stedet eller fjerndiagnose og problemløsning.
Niveau 3 support (teknik/fejlfinding)	Produktsupport-medarbejdere kan fejlfinde vanskelige problemer, når de får adgang til detaljerede teknik- og fejlfindingslogs.

Grundlæggende data fra printenheden komprimeres, overføres, opbevares og arkiveres i et ISO-27001-certificeret Xerox®-datacenter og opbevares iht. Xerox®-opbevaringspolitikkerne.

De arbejdsprocesser og den praksis, der understøtter og beskytter Xerox®-administrationens Remote Services-softwaresystemer, er baseret på ITIL's bedste praksis og Xerox-politikker for informationssikkerhed, der er baseret på ISO 27001-standarden. Kunderne kan være sikre på, at administrationen af dataintegritet, fortrolighed og beskyttelse er på højde med den bedste praksis.

Oplysninger om teknologi

Dette afsnit indeholder yderligere tekniske oplysninger, som typisk kræves af IT-teams og sikkerhedsmedarbejdere med det formål at styre risici i forbindelse med opnåelse af sikre udviklingsmetoder, hvilket gør det muligt at certificere printenheder og Device Management-applikationer til brug i kundens netværksmiljø.

Softwaredesign

Vores engagement i Xerox®-produktsikkerhed starter tidligt i produktudviklingen med bedste praksis i branchen for sikker kodning, omfattende test og analyse for at eliminere sårbarheder. Xerox® deltager aktivt i certificeringspraksis, f.eks. fælles kriterier, og er aktiv i nye standarder, f.eks. P2600-arbejdsgruppen og SDLC (Security Development Lifecycle).

Funktionalitet

Xerox® Remote Services udfører følgende typer af funktioner på et netværk:

Udrulningsmetode	Anvendt applikation	Dataflow på netværk	Funktionalitet indført på et netværk
Device Direct	Ingen	Intern	Xerox®-printenhed forsøger at registrere en Web Proxy Server (automatisk eller orienteret mod en specifik adresse)
		Intern	Xerox®-printenheder kan programmeres til at generere anmodninger til en SMTP-server (Simple Mail Transport Protocol) om at sende advarselsnotifikationer pr. e-mail til en defineret modtagerliste
		Eksternt til netværk	Xerox®-printenhed passerer virksomhedens firewall for at få adgang til internettet (HTTPS via port 443)
		Eksternt til netværk	Xerox®-printenhed godkender med sit certifikat til den eksterne Xerox Communication Server, før der overføres nogen dataattributter
		Eksternt til netværk	Xerox®-printenhed overfører automatisk sine attributdata gennem en krypteret kanal (HTTPS via port 443) til Xerox® Communication Servers på et bestemt tidspunkt hver dag eller ved kundehenvendelse.
		Eksternt til netværk	Xerox®-printenhed forespørger automatisk Xerox® Communication Servers gennem en krypteret kanal (HTTPS via port 443) på et bestemt tidspunkt hver dag om en liste over handlinger til udførelse (f.eks. send faktureringsdata nu, tilføj service osv.)
		Eksternt til netværk	Envejs on-demand overførsel af Xerox®-printenhedens tekniske logdata gennem en krypteret kanal (HTTPS via port 443) til Xerox® Communication Server

Udrulningsmetode	Anvendt applikation	Dataflow på netværk	Funktionalitet indført på et netværk
Device Management-applikationer	Centre Ware® Web	Intern	Hver app registrerer en Web Proxy Server (automatisk eller orienteret til en specifik adresse)
		Intern	Hver app henter printenheders funktionalitet på tværs af printerparken via SNMP
		Intern	Hver app henter printenheders konfiguration på tværs af printerparken via SNMP
		Intern	Hver app henter printenheders status på tværs af printerparken via SNMP
		Intern	Hver app henter printenheders forbrugsvare-data på tværs af printerparken via SNMP
		Intern	Hver app kan genstarte en printenhed via SNMP eller via printenhedens web UI
		Intern	Hver app kan sende en testside til en specifik printenhed
		Intern	Hver app kan opstarte en printenheds webside
		Ekstern **(kun udgående)**	Hver app passerer virksomhedens firewall for at få adgang til internettet (HTTPS via port 443)
		Ekstern **(kun udgående)**	Hver app godkender med sit certifikat til den eksterne Xerox Communication Server, før der overføres nogen dataattributter
		Ekstern **(kun udgående)**	Hver app overfører automatisk printenhedens attributdata gennem en krypteret kanal (HTTPS via port 443) til Xerox® Communication Servers på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Hver app forespørger automatisk Xerox® Communication Servers gennem en krypteret kanal (HTTPS via port 443) på et bestemt tidspunkt hver dag om en liste over handlinger til udførelse
		Intern	Hver Xerox® Device Agent-app registrerer en Web Proxy Server (automatisk eller orienteret mod en specifik adresse)
		Intern	Hver Xerox® Device Agent-app henter printenhedernes funktionalitet på tværs af printerparken via SNMP
		Intern	Hver Xerox® Device Agent-app henter printenhedernes konfiguration på tværs af printerparken via SNMP
		Intern	Hver Xerox® Device Agent-app henter printenhedernes status på tværs af printerparken via SNMP
		Intern	Hver Xerox® Device Agent-app henter printenhedernes forbrugsdata på tværs af printerparken via SNMP
		Intern	Hver Xerox® Device Agent-app kan anmode enheden om at printe en konfigurationsrapport

Udrulningsmetode	Anvendt applikation	Dataflow på netværk	Funktionalitet indført på et netværk
Device Management-applikationer	Xerox® Device Agent Partner Edition til overvågning af netværkstilslutte de printenheder	Intern	Hver Xerox® Device Agent-app kan starte en printenheds webside
		Intern	Hver Xerox® Device Agent-app kan opgradere printenheders software via printjobafsendelse. (.DLM-fil via port 9100)
		Ekstern (**kun udgående)**	Hver Xerox® Device Agent-app passerer virksomhedens firewall for at få adgang til internettet (HTTPS via port 443)
		Ekstern **(kun udgående)**	Hver app godkender med sit certifikat til den eksterne Xerox Communication Server, før der overføres nogen dataattributter
		Ekstern **(kun udgående)**	Hver Xerox® Device Agent-app overfører automatisk printenhedens attributdata gennem en krypteret kanal (HTTPS via port 443) til Xerox® Communication Servers på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Hver Xerox® Device Agent-app forespørger automatisk Xerox® Communication Servers gennem en krypteret kanal (HTTPS via port 443) på et bestemt tidspunkt hver dag om en liste over handlinger til udførelse
	Xerox® Device Manager til overvågning af netværkstilslutte de printenheder	Intern	Xerox® Device Manager/Xerox® Device Agent-apps registrerer en Web Proxy Server (automatisk eller orienteret mod en specifik adresse)
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps henter printenhedernes funktionalitet på tværs af printerparken via SNMP
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps henter printenhedernes konfiguration på tværs af printerparken via SNMP
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps henter printenhedernes status på tværs af printerparken via SNMP
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps henter printenhedernes forbrugsdata på tværs af printerparken via SNMP
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps kan anmode enheden om at printe en konfigurationsrapport
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps kan starte en printenheds webside
		Intern	Xerox® Device Manager/Xerox® Device Agent-apps kan opgradere printenhedens software via printjob-afsendelse
		Intern	Xerox® Device Manager-appen understøtter SNMPv3-kommunikation med printenheder

Udrulningsmetode	Anvendt applikation	Dataflow på netværk	Funktionalitet indført på et netværk
Device Management-applikationer		Intern	Xerox® Device Manager-appen kan foretage ændringer i printenhedens konfiguration via SNMP og web UI
		Intern	Xerox® Device Manger-appen modtager jobbaserede regnskabslogs fra visse Xerox® MFP'ere
		Intern	Xerox® Device Manager-appen administrerer/håndhæver printkontrolpolitikker
		Ekstern **(kun udgående)**	Xerox® Device Manager/Xerox® Device Agent-apps passerer virksomhedens firewall for at få adgang til internettet (HTTPS via port 443)
		Ekstern **(kun udgående)**	Hver app godkender med sit certifikat til den eksterne Xerox Communication Server, før der overføres nogen dataattributter
		Ekstern **(kun udgående)**	Xerox® Device Manager/Xerox® Device Agent-apps overfører automatisk printenhedens data til Xerox® Communication Servers gennem en krypteret kanal (HTTPS via port 443) på et bestemt tidspunkt hver dag
		Ekstern **(kun udgående)**	Xerox® Device Manager/Xerox® Device Agent-apps forespørger automatisk Xerox® Communication Servers gennem en krypteret kanal (HTTPS via port 443) på et bestemt tidspunkt hver dag om en liste over handlinger til udførelse

Simple Network Management Protocol (SNMP)

SNMP (Simple Network Management Protocol) er det mest udbredte værktøj til netværksadministration til kommunikation mellem netværksadministrationssystemer og netværksprintere. Device Management-applikationerne bruger SNMP under registreringshandlinger til at hente detaljerede oplysninger om de printenheder, der findes på netværket. Xerox® Device Management-applikationer understøtter protokollerne SNMP v1/v2 og v3. Se certificeringsvejledningen til den pågældende Xerox® Device Management-applikation for at forstå specifikke oplysninger.

SNMP v3 Framework understøtter flere sikkerhedsmodeller, der kan eksistere samtidigt på en SNMP-enhed. SNMPv3 indeholder en strammere sikkerhed ved at føje kryptografisk sikkerhed til SNMPv2. SNMPv3 er desuden bagudkompatibel med tidligere versioner og bruges i vid udstrækning på en række robuste netværk.

Xerox® Device Management-applikationer (Centre Ware® Web/Xerox® Device Manager) kan kommunikere med enhedsplatforme, der overholder FIPS 140-2 i deres implementering af SNMPv3.

Xerox® Device Management-applikationerne benytter ikke tjenesten Windows SNMP eller Windows SNMP Trap. Hvis disse tjenester er blevet installeret på et tidligere tidspunkt, **skal** de deaktiveres på den pc eller server, hvor Xerox® Device Management-applikationen er installeret.

Xerox® Device Management-applikationer benytter en Xerox-udviklet SNMP-agent, der:

- Indeholder en speciel kodnings-/afkodningsmekanisme
- Er fuldstændig .NET-styret
- Bruger .NET-runtime eksekverbare filer, der giver øget sikkerhed for at forhindre angreb på softwarens sårbarhed, f.eks. ugyldig pointermanipulation, bufferoverløb og boundkontrol.

Xerox® Device Management-applikationerne benytter de sikkerhedsfunktioner, der findes i Windows-operativsystemet (OS) inklusive:

- Brugerautentifikation og autorisation
- Servicekonfiguration og administration
- Udrulning og administration af gruppepolitikker

Windows Firewall til internetforbindelse (ICF) inklusive:

- Indstillingerne for sikkerhedslogføring
- ICMP-indstillinger

Xerox® Device Management-applikationer: **Xerox® Device Agent, Xerox® Device Agent Partner Edition eller Xerox® Device Manager** bruger SQL CE-applikationen Microsoft® SQL Server

Xerox® Device Management-applikationen kan konfigureres til at benytte yderligere sikkerhedsfunktioner fra Microsoft® SQL Server-applikationen inklusive:

- Aktivering af brugerkontoregistrering

- Kryptering af Domain Name System (DNS)
- Begrænsning af brugerkontorettigheder for adgang til databasen (dvs. databaseejerrettigheder)
- Implementering af brugerdefinerede portnumre

Det kræver en Xerox-registreringsnøgle og en gyldig Xerox-konto for at overføre data til de eksterne Xerox® Communications Servers.

Xerox® Device Management-applikationernes eksterne kommunikation kan blive påvirket af Windows Internet Connection Firewall. (Vi **anbefaler**, at kunderne godkender Xerox-URL'en i deres firewall og angiver den IP-adresse, der kan få adgang til URL'en.)

Xerox® Device Management-applikationerne kører som baggrundsprocesser med lokale systemkonto-brugeroplysninger for automatisk forespørgsel til netværkets printenheder via SNMP og overfører regelmæssigt attributter om printenheden til Xerox® Communications Servers

Adgangen til Xerox® Device Manager-applikationens (XDM) brugerflade (UI) og funktioner kontrolleres via følgende rollebaserede rettigheder (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-kundegrupper).

Brugernavne og adgangskoder til applikationerne passerer ikke netværket; i stedet benyttes adgangstokens (af Windows® OS-design).

Xerox® Device Manager-applikationer (XDM) giver kontrolbaseret sikkerhed ved printafsendelse ved at begrænse jobs baseret på farveforbrugs-politik, dokumenttype, jobpris, tidspunkt på dagen, adgangskontrol for brugergrupper, duplexpolitik, tilladte jobkopier og printkvoter.

Bemærkninger: En Xerox® Remote Services-applikations brug af SNMP burde ikke udgøre en sikkerhedsrisiko for kundes IT-miljø, fordi al SNMP-baseret trafik, der genereres eller bruges af disse applikationer opstår inden for kundens intranet bag en firewall. Tjenesten Windows SNMP og Windows SNMP Trap er ikke aktiveret i Windows OS som standard.

Virksomhedens sikkerhedstilstand

Ud over eventuelle planlagte synkroniseringer fra Xerox® Device Management-applikationer til Xerox® Services Manager, foretages der en daglig synkronisering som standard. Virksomhedens to sikkerhedstilstande er **Normal** og **Spærret tilstand.**

I **normal** tilstand kontakter Device Management-applikationen dagligt Xerox® Services Manager, når alle andre planlagte synkroniseringer er slået fra ***(anbefalet tilstand***).

I **spærret tilstand** er der ingen kommunikation med Xerox® Services Manager ud over printerrelateret datasynkronisering. Ændringer i denne indstilling skal foretages på stedet. (***Datasynkronisering*** sikrer, at det er de samme printeroplysninger, der sendes af Xerox® Device Management-applikationen, som modtages af Xerox® Services Manager).

Xerox® Device Management-applikationen kontakter som standard Xerox® Services Manager dagligt og tillader administratorer at fjernredigere indstillinger, så der ikke er behov for servicebesøg på stedet. Vi anbefaler, at denne indstilling ikke ændres. Hvis en kunde begrænser Xerox-medarbejdernes mulighed for at udføre fjernsupport, kan enhedens kommunikation med Xerox® Services Manager låses undtagen synkroniseringen af printerdata. I denne tilstand rapporterer applikationen ikke computerens eller printerens IP-adresser eller stedets indstillinger til Xerox® Services Manager, og alle ændringer af indstillinger kræver et besøg på stedet.

Bemærk: Hvis Xerox® Device Agent ikke indeholder fanen Corporation Security Mode (Virksomhedens sikkerhedstilstand), kører den i Normal tilstand.

Protokoller, porte og andre relaterede teknologier

Følgende tabel identificerer de protokoller, porte og teknologier, der benyttes i Xerox® Remote Services:

Portnummer	Protokol	Beskrivelse af anvendelse	Dataflow på netværket
Afhængig af øvre-lags protokoller	**Internet Protocol (IP)**	**Underliggende transport for al datakommunikation**	**Intern + ekstern (kun udadgående)**
Ikke relevant	Internet Control Message Protocol (ICMP)	Registrering af printenhed + fejlfinding	Intern
25	Simple Mail Transport Protocol (SMTP)	Printenhed + Remote Proxy App e-mail-notifikation advarsler	Intern
53	Domain Name Services (DNS)	Benyttes til DNS-baseret registrering af printenhed	Intern
80	Hyper Text Transport Protocol (HTTP)	Forespørgsler til printenheds webside + forespørgsler til Device Management-applikations webside	Intern
135	Remote Procedure Call (RPC)	Registrering af printenhed	Intern
137, 139	NetBIOS	Registrering af printserver	Intern
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Branchestandard protokol bruges til at registrere netværkstilsluttede printenheder + Hente status, tællere & forbrugsvaredata + Hente og anvende printenheds konfiguration. Default community navne = “public” (GET), “private” (SET)	Intern
162	SNMP traps	Default community navn = “SNMP_trap”	Intern
389	Lightweight Direct Access Protocol (LDAP)	Registrering af printenhed via MS Active Directory Partition enumeration + Scanningsservice konfigurationssæt + Active Directory kundeimport + Kundegruppe konfigurationer	Intern
443	Hyper Text Transport Protocol Secure (HTTPS)	Forespørgsler til printenheds sikre webside (hvis konfigureret) + forespørgsler til Remote Proxy-apps sikre webside (hvis konfigureret) + Overførsel af printenheds data tilbage til Xerox® Communication Servers + printkontrollers kommunikation tilbage til Xerox® Device Manager	Intern + ekstern (kun udadgående)

Portnummer	Protokol	Beskrivelse af anvendelse	Dataflow på netværket
452	Netware Service Advertising Protocol (SAP)	Registrering af printenhed ved brug af Novell Server forespørgsler via IPX	Intern
515, 9100, 2000, 2105	TCP/IP LPR & Raw Port printjob afsendelse	Printenhed softwareopgradering + print testside diagnostik	Intern
631	Internet Printing Protocol (IPP)	Registrering af printenhed	Intern

Bedste praksis for sikkerhed

Hold altid printenheder opdaterede med den seneste firmware/software. Benyt enten printenhedens webbaserede brugerflade (UI) eller den applikation til printeradministration, der stilles til rådighed af Xerox® og andre printerleverandører for at opgradere printenhedens firmware/software.

Deaktiver ikke-anvendte porte og protokoller på printenheder, hvor det er muligt. Dette gøres typisk via den webbaserede brugerflade (UI) på printenheder i kontorklassen og den lokale brugerflade (UI) på printenheder i produktionsklassen.

Benyt kontrolrelaterede funktioner for brugeradgang på printenheder, hvis tilgængelig. Dette gøres typisk via den webbaserede brugerflade (UI) på printenheder i kontorklassen og den lokale brugerflade (UI) på printenheder i produktionsklassen.

Benyt sikre protokoller, når det er muligt. Dette gøres typisk via den webbaserede brugerflade (UI) på printenheder i kontorklassen og den lokale brugerflade (UI) på printenheder i produktionsklassen.

Aktiver sikkerhedsfunktioner indbygget i enheden (f.eks. billedoverskrivning, disk-kryptering, sikker print osv.)

Sørg for, at virksomhedens firewall kan route HTTPS-pakker via port 443 iht. virksomhedens sikkerhedspolitik.