Remote Services @ Xerox

Whitepaper over beveiliging

Versie 4.0

Maart 2022

IS 614672/IS 514590

Inhoudsopgave

1. Algemeen doel en publiek

Het whitepaper over beveiliging van Remote Services @Xerox wordt geleverd om klanten te helpen de oplossing voor beveiligde remote services te begrijpen en te implementeren die het beste werkt met hun netwerkconstructie en informatiebeveiligingsbeleid. Houd er rekening mee dat wijzigingen in de internetfirewall, webproxyservers of andere beveiligingsgerelateerde netwerkinfrastructuur van de klant nodig kunnen zijn om de meest veilige configuratiemethode te garanderen.

De doelgroep voor dit document omvat technische leveranciers, netwerkbeheerders en netwerkbeveiligingsprofessionals die geïnteresseerd zijn in de mogelijkheden van remote services de beveiligingsimplementatie van deze functies.

We raden aan het document in zijn geheel te beoordelen om het gebruik van producten en diensten van Xerox® binnen de netwerkomgeving van een klant te certificeren.

2. Waardepropositie

Wij bieden een veilige en beveiligde manier voor het verzenden van apparaatgegevens naar ons ISO-gecertificeerde systeem om gemeenschappelijke taken te automatiseren en een betere service en ondersteuning te bieden.

- De rapportage van de factureringsmeter is geautomatiseerd en nauwkeurig.
- Het programma voor het automatisch aanvullen van voorraden biedt toner op basis van de gerapporteerde tonerniveaus van de printer, zodat het niet nodig is om de voorraad bij te houden of om extra voorraden aan te vragen.
- Het verzenden van diagnostische informatie stelt ons in staat om uw apparaat beter te ondersteunen, waardoor het probleem vaak sneller kan worden opgelost.
- Bepaalde printermodellen kunnen controleren op belangrijke software-updates en de updates via programmacode installeren zonder tussenkomst van de klant.Zie Opmerking
- Onze beheerde diensten bieden ook een manier om naast afdrukapparaten van Xerox ook afdrukapparaten met een ander merk dan Xerox te beheren.
- Dankzij deze diensten kunnen onze klanten hun tijd efficiënter besteden.

Dit alles gebeurt met veiligheid in het achterhoofd.

Opmerking: Deze optie kan worden uitgeschakeld voor omgevingen waar klanten certificeren naar een ingestelde softwareversie en printsoftware willen beheren wanneer updates plaatsvinden. Dit kan worden gedaan zonder de resterende mogelijkheden voor remote services uit te schakelen.

3. Remote Services

Informatie is kapitaal en beveiliging is van het grootste belang voor alle bedrijfsmiddelen van de organisatie, inclusief netwerkgebonden multifunctionele afdrukapparaten (MFP's). Tegenwoordig vormt het beheer van een vloot multifunctionele afdrukapparaten met garantie van een aanvaardbaar beveiligingsniveau een reeks unieke uitdagingen die vaak over het hoofd worden gezien. We begrijpen deze complexiteit en spelen in op de beveiligingsbehoeften van onze klanten. Producten en systemen van Xerox®, en remote services zijn ontworpen om veilig te integreren met de bestaande workflows van onze klanten en tegelijkertijd gebruik te maken van de nieuwste veilige technologieën.

Standaard worden er geen klantbeelden van print-, fax-, scan-, kopieeracties of andere gevoelige informatie naar onze servers verzonden.

De in de VS gevestigde Xerox-servers voldoen aan strenge beveiligingseisen voor informatiebeveiligingsbeheer. Onze datacenters en applicaties voor remote services handhaven de jaarlijkse compliancevereisten van de 'Statement on Standards for Attestation' (SSAE) No-16, Sarbanes-Oxley Act (SOX) en zijn ISO 27001:2013 gecertificeerd.

4. Implementatiemodellen

Klanten kunnen kiezen tussen de volgende Xerox® Remote Services-implementatiemodellen, alle even veilig:

- **Combinatiemodel** –***(Voorkeursmodel)*** Implementatie van het Device Direct en de Device Management Application Model samen is ideaal, omdat het de meest robuuste gegevensverzameling en mogelijkheden voor apparaatbeheer biedt.

- **Device Direct-model** - Met Device Direct kunnen afdrukapparaten rechtstreeks via internet communiceren met de Xerox®-communicatieservers op afstand via de firewall van de klant ter ondersteuning van Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) en diagnostische rapportage van apparaten.Dit implementatiemodel biedt een set gegevenselementen in de standaard payload om apparaatfouten, waarschuwingen, tellers, HFSI (High Frequency Service Items) en andere printerkenmerken op te nemen.
- **Applicatiemodel voor het beheer van apparaten** - Xerox®-applicaties voor apparaatbeheer kunnen in het netwerk van een klant worden geïmplementeerd om een reeks gegevensattributen van afdrukapparaten te verzamelen ter ondersteuning van 'Automatic Supplies Replenishment' (ASR - Automatische aanvulling van verbruiksartikelen), 'Automatic Meter Reads' (AMR - Automatische meterlezing) en diagnostische rapportage van apparaten.Printerattributen worden verzameld en vervolgens veilig verzonden naar de remote servers van Xerox.Gegevensattributen van Xerox-afdrukapparaten en niet-Xerox-afdrukapparaten kunnen worden gecommuniceerd als onderdeel van dit implementatiemodel.

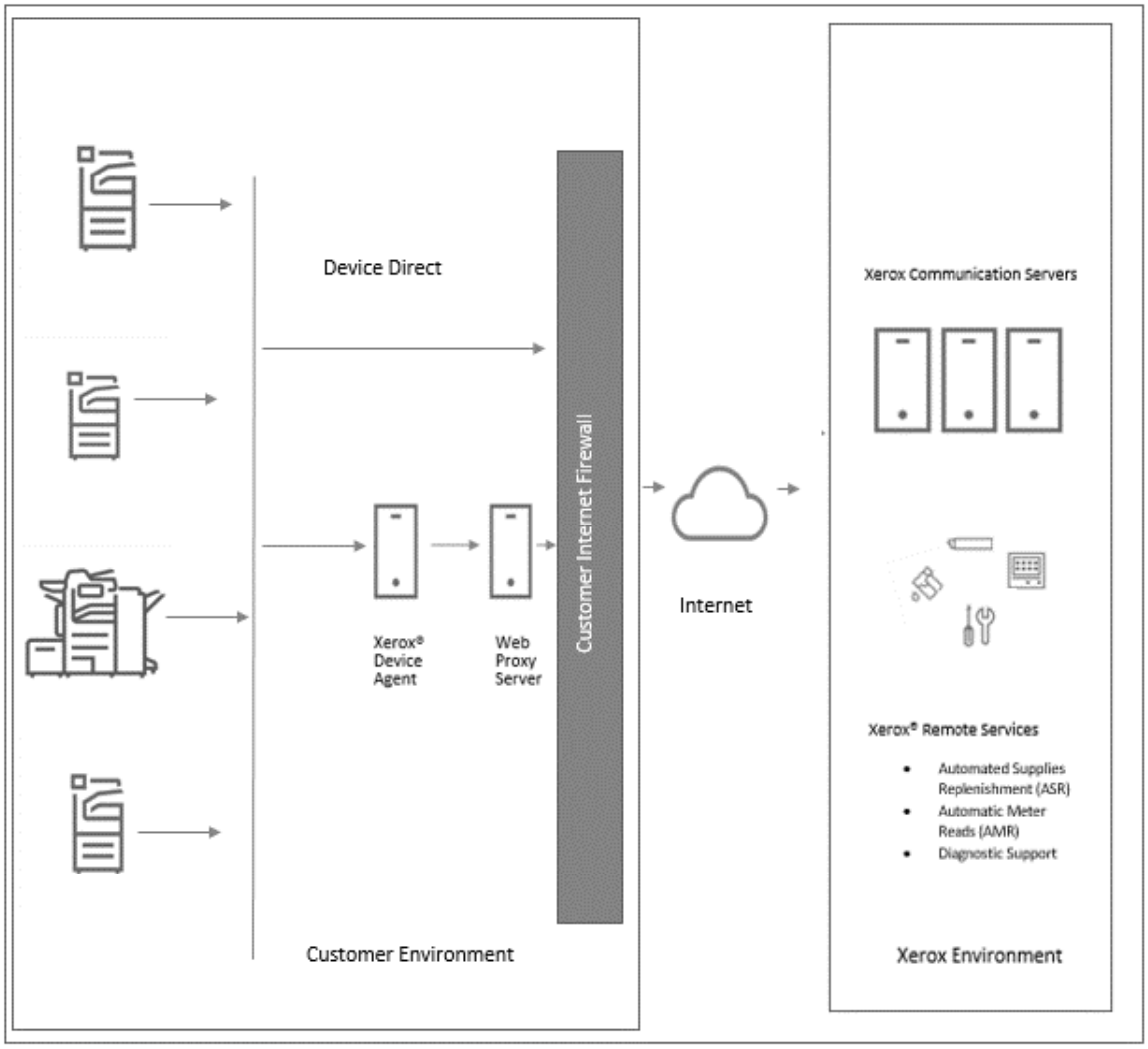
Alle implementatiemodellen voor Xerox® Remote Services zijn even veilig en maken gebruik van de nieuwste webgebaseerde protocollen en poorten volgens de industrienorm om een veilig, versleuteld kanaal te creëren bij het extern verzenden van printerkenmerken naar de remote servers van Xerox in onze dubbel beveiligde datacenters.

Het gekozen implementatiemodel is afhankelijk van het type print service oplossing van onze klanten, het informatiebeveiligingsbeleid en de regels voor de overdracht van de gegevenskenmerken van de printer.

Combinatie-implementatiemodel (voorkeur)

Het Combinatie-implementatiemodel wordt ingezet wanneer een klant meerdere soorten onderhoudsovereenkomsten van Xerox aanschaft voor zijn afdrukapparaten en voor een robuustere oplossing voor remote services. Wanneer een afdrukapparaat van Xerox® in het begin op een netwerk is geïnstalleerd, zorgen de remote services van Xerox er standaard voor dat het afdrukapparaat automatisch probeert te communiceren met onze communicatieservers via een beveiligde, geverifieerde verbindingsmethode.

Afbeelding 1



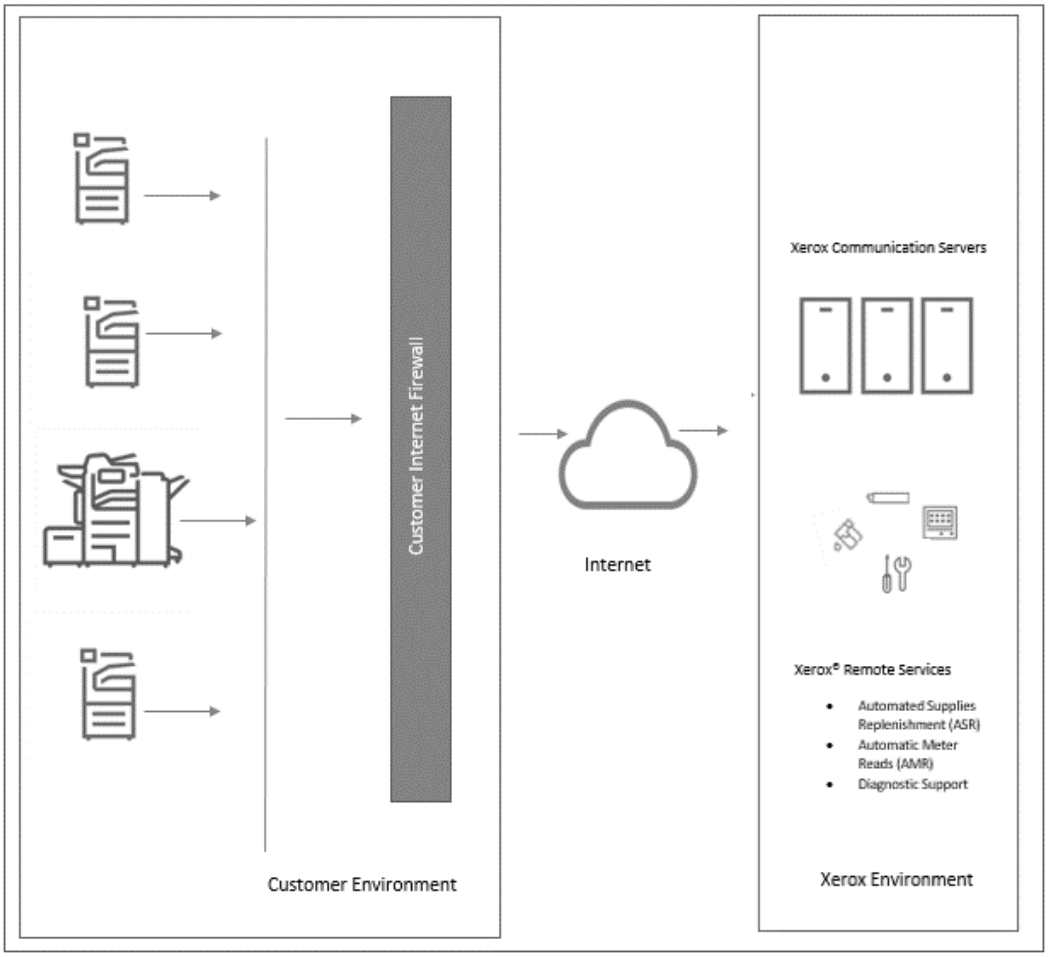
Combination Deployment Model

Device Direct-implementatiemodel

Xerox® -apparaten geschikt voor remote services maken gebruik van een Transport Layer Security (TLS) 1.2-protocolverbinding via de beveiligde standaardpoort 443 om te communiceren met onze beveiligde servers.

- Afdrukapparaten binnen de klantomgeving initiëren alle communicatie met de communicatieservers. Op de site zijn standaard firewallconfiguraties vereist om communicatie mogelijk te maken.
- Er moet een geldige URL voor de communicatieservers worden gebruikt (*.xerox.support.com) om afdrukapparaten te verifiëren bij de infrastructuur van Xerox
- Het apparaat vraagt een registratie aan bij de communicatieservers met de juiste inloggegevens voor certificaatverificatie.
- De communicatieservers valideren de door de afdrukapparaten aangeleverde referenties en accepteren de aanvragen.
- De communicatieservers bevinden zich achter een veilige firewall en zijn niet toegankelijk vanaf het internet.

Afbeelding 2



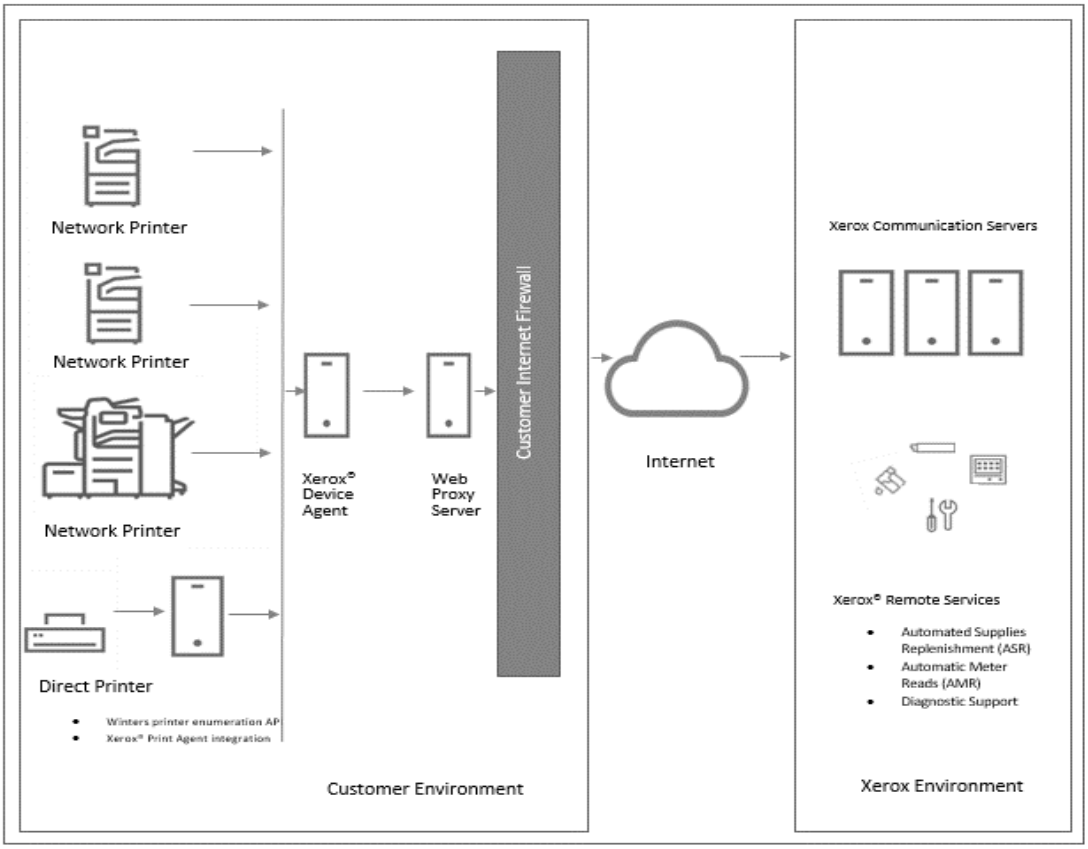
Device Direct Deployment Model

Implementatiemodel voor apparaatbeheer

De applicaties voor apparaatbeheer (d.w.z. **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition en Xerox Device Manager)** maken gebruik van een Transport Layer Security (TLS) 1.2 protocol-verbinding via de beveiligde standaardpoort 443 om extern te communiceren met de communicatieservers.Extra functies worden gebruikt om de veiligheid van dit kanaal te verbeteren. Deze worden vastgesteld tijdens de eerste installatie van de applicaties voor apparaatbeheer, waaronder:

- De applicatie voor Apparaatbeheer binnen de klantomgeving initieert alle communicatie met de communicatieservers. Op de site zijn standaard firewallconfiguraties vereist om communicatie mogelijk te maken.
- De communicatieservers bevinden zich achter een veilige firewall en zijn niet toegankelijk vanaf het internet.
- De applicatie voor Apparaatbeheer vraagt een registratie aan bij de externe servers met behulp van de juiste referenties voor certificaatverificatie.
- De communicatieservers valideren de door de afdrukapparaten aangeleverde referenties en accepteren de aanvragen.
- De applicatie voor Apparaatbeheer authenticeert de communicatieservers en activeert de dienst.

Afbeelding 3



Device Management Application Deployment Model

5. Datatransmissie en payloads

Gegevensbronnen

De gegevenskenmerken van het afdrukapparaat die als onderdeel van de overgedragen payload worden verzonden, zijn afkomstig van de volgende bronnen:

- Xerox® Office-netwerkprinters
- Non-Xerox netwerkprinters
- Xerox® Production-printers
- Applicaties voor Xerox®-apparaatbeheer

Opmerking: Niet alle Xerox Office- en Xerox Production-afdrukapparaten zijn geschikt voor Xerox Remote Services. U vindt hier een volledige lijst van geschikte producten.De kenmerken van het afdrukapparaat verschillen per product en de implementatieoplossing van Xerox® Remote Services.

Xerox® Office-apparaten

Tabel 1 identificeert de kenmerken van apparaatgegevens die kunnen worden verzonden voor Xerox® Office-producten die geschikt zijn voor Xerox Remote Services.

Gegevens-kenmerken	Gedetailleerde beschrijving van gegevenskenmerken
Identiteit afdrukapparaat	Bevat model, module firmwareniveaus, serienummers van de module, installatiedata van de module, licentiegegevens en locatie, indien beschikbaar.
Netwerkadres van afdrukapparaat	Inclusief Media Access Control (MAC)-adres, subnetadres.
Eigenschappen van afdrukapparaat	Inclusief gedetailleerde configuratie van hardwarecomponenten, gedetailleerde configuratie van softwaremodules, ondersteunde functies/services, enz.
Status afdrukapparaat	Bevat actieve statussen, aantal storingsdata, DFE-gebeurtenislogboek, gegevensoverdrachtshistorie
Tellers afdrukapparaat	Omvat facturatiemeters, printgerelateerde tellers, kopieergerelateerde tellers, tellers gerelateerd aan grote opdrachten, productspecifieke tellers, tellers gerelateerd aan scannen naar-bestemming op low-end productiemodellen, enz.
Toebehoren afdrukapparaat	Omvat fabrikant, model, serienummer, naam, type, niveau, capaciteit, status, levensduurtellers, enz.
Gedetailleerd gebruik afdrukapparaat	Omvat HFSI-gegevens, NVM-gegevens, vervanging van onderdelen, DFE-logboeken, gedetailleerde diagnostische gegevens, foutoplossing.
Engineering / debugging	Bevat niet-gestructureerde, gedetailleerde debug-gerelateerde gegevens die alleen bedoeld zijn voor ondersteuning op het derde niveau.
Klanttakengerelateerd	Printproducten van Xerox® Production bieden de mogelijkheid om taakgerelateerde gegevens te reproduceren ter ondersteuning van geëscaleerde ondersteuningsscenario's via versleutelde PostScript naar Xerox. De klant kan zelf bepalen of hij deze functie wil activeren of niet. Als de klant ervoor kiest om functiegerelateerde gegevens (d.w.z. gecodeerde PostScript) terug te sturen naar Xerox, worden die gegevens verwerkt in overeenstemming met het beleid en de normen van Xerox voor informatiebeveiliging (IS).

Onze afdrukapparaten voor kantoor verzenden de gegevenskenmerken van het apparaat in een XML-formaat (eXtensible Markup Language) met behulp van een gecomprimeerd zip-bestand. Eenmaal geverifieerd, wordt elk bestand vervolgens via een versleuteld kanaal naar de communicatieservers verzonden.

Xerox® Production-apparaten

Tabel 2 identificeert de kenmerken van apparaatgegevens die kunnen worden verzonden voor Xerox® Office-producten die geschikt zijn voor Xerox Remote Services.

	Beschrijving
Identiteit afdrukapparaat	Omvat model, firmwareniveau, serienummers van module en installatiedatum.
Netwerkadres van afdrukapparaat	Inclusief Media Access Control (MAC)-adres, subnetadres.
Eigenschappen van afdrukapparaat	Omvat gedetailleerde configuratie van hardwarecomponenten, gedetailleerde configuratie van softwaremodules, ondersteunde functies/services, energiebesparende modi, enz.
Status afdrukapparaat	Omvat algemene status, gedetailleerde waarschuwingen, geschiedenis van laatste 40 storingen, gegevens over papierstoringen, etc.
Tellers afdrukapparaat	Omvat facturatiemeters, printgerelateerde tellers, kopieergerelateerde tellers, faxgerelateerde tellers, tellers gerelateerd aan grote opdrachten, scan-naar-bestemming-gerelateerde tellers, gebruiksstatistieken, enz.
Toebehoren afdrukapparaat	Omvat de naam van het verbruiksartikel, het type (bijv. beeldkwaliteit, afwerking, papiermedia), niveau, capaciteit, status, grootte, enz.
Gedetailleerd gebruik afdrukapparaat	Omvat gedetailleerde printgerelateerde tellers, inschakelstatussen, gedetailleerde vervangingshoeveelheden van Customer Replaceable Units (CRU - door de klant vervangbare onderdelen), gedetailleerde CRU-storingsgegevens en -distributies, ingesloten functiegebruik van Optical Character Recognition (OCR), distributie van afdruklengte, distributie van papierladegebruik, geïnstalleerde media, distributie van mediatypen, distributie van mediagrootte, distributie van documentlengte, vastgesteld aantal, HFSI-gegevens, NVM-gegevens, distributie, gemarkeerde pixeltellingen, gemiddelde gebiedsdekking per kleur, storingen/papierstoringen, gedetailleerde scangerelateerde tellers.
Engineering / debugging	Bevat gedetailleerde foutopsporingsinformatie die gegevens kan bevatten die buiten de hierboven vermelde gegevensverzameling vallen. Deze gegevens kunnen PII omvatten, zoals gebruikersnamen, e-mailadressen en taakgegevens. Deze gegevens worden alleen verzonden met uitdrukkelijke toestemming van de klant en zijn alleen bedoeld voor geëscaleerde technische ondersteuning voor probleemoplossing.

Onze afdrukapparaten voor productie verzenden de gegevenskenmerken van het apparaat in een XML-formaat (eXtensible Markup Language) met behulp van een gecomprimeerd zip-bestand. Eenmaal geverifieerd wordt elk bestand vervolgens via een versleuteld kanaal verzonden naar de servers voor remote services.

Opmerking: Het bestand en de inhoud van de geïdentificeerde gegevens variëren afhankelijk van het productmodel.

Applicaties voor Xerox®-apparaatbeheer

Er zijn verschillende applicatiemogelijkheden voor apparaatbeheer beschikbaar op basis van de netwerkomgeving van de klant en de behoefte aan afdrukapparaatbeheer. Deze zijn alle even veilig en beschikken over robuuste mogelijkheden voor het beheer van afdrukapparaten.

Hieronder volgt een lijst met toepassingen voor apparaatbeheer: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition en Xerox Device Manager.

Elke applicatie synchroniseert standaard ten minste dagelijks met de beveiligde communicatieservers. Om een maximale beveiliging van uw gegevens te garanderen, worden de communicatieservers gehost in een faciliteit die voldoet aan ISO 27001. Verzonden gegevens zijn voornamelijk printerspecifieke facturatietellers, voorraadniveaus en printerwaarschuwingen. Gegevens worden gecomprimeerd, versleuteld en beschermd door verschillende mechanismen:

- Xerox Device Management Application initieert elk contact met de Xerox-communicatieservers, standaard firewallconfiguraties in de klantomgeving zijn vereist om communicatie mogelijk te maken.
- Voor Xerox Device Management Applications is een geldige proxy vereist, indien een proxy nodig is voor internetcommunicatie.
- Xerox-communicatieservers zitten achter een veilige firewall in de Xerox-omgeving en zijn niet toegankelijk vanaf het internet.
- De gebruikersinterface van de Xerox-communicatieserver moet worden geverifieerd. De hostinformatie van Xerox Device Management-applicatie wordt opgeslagen in een account dat specifiek is voor de klantlocatie en de toegang tot die accountgegevens in Xerox-communicatieservers is beperkt tot accountmanagers van Xerox-communicatieservers.
- Alle communicatie van de Xerox-communicatieserver wordt geregistreerd en kan worden bekeken.
- Gegevens die naar uw aangesloten afdrukapparaten worden verzonden, bestaan, indien ingeschakeld, voornamelijk uit externe commando's waarmee een accountondersteuningsbeheerder de uitvoering van Xerox Device Management-applicatiecommando's kan aanvragen tijdens geëscaleerde ondersteuningsscenario's.
- Verzoeken hebben voornamelijk betrekking op firmware-updates, herstarten van de printer, afdrukken van testpagina's en vernieuwen van de huidige apparaatstatus.
- De Xerox-applicatie voor apparaatbeheer peilt periodiek de Xerox-communicatieserversaccount voor opdrachtverzoeken.
- Operationele resultaten van commandoverzoeken worden verzonden naar de Xerox-communicatieservers waar ze vervolgens worden beoordeeld.

Opmerking: De software-installatie vereist een eenmalige registratie. Deze registratiegegevens bevatten een veld voor de locatie van het apparaat en contact e-mail.

De Xerox-applicaties voor apparaatbeheer **(d.w.z. Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition en Xerox Device Manager** verzenden de gegevens van afdrukkenmerken in eXtensible Markup Language (XML) - indeling met behulp van een gecomprimeerd .zip-bestand. Het bestand wordt vervolgens versleuteld en via versleutelde kanalen naar de externe communicatieservers verzonden.

Tabel 3 identificeert de lijst met kenmerken en beschrijvingen van apparaatgegevens die kunnen worden verzonden via de Xerox® Device Mgmt.-app.

Gegevenskenmerken	Gedetailleerde beschrijving van gegevenskenmerken
Identiteit afdrukapparaat	Bevat fabrikant, model, beschrijving, firmwareniveau, serienummer, assettags, systeemnaam, contact, locatie, beheerstatus werkstation (desktop), fax-/telefoonnummer en wachtrijnaam.
Netwerkadres van afdrukapparaat	Inclusief MAC-adres, IP-adres, DNS-naam, subnetmasker, IP-standaardgateway, laatst bekende IP-adres, IP-adres gewijzigd, tijdzone, IPX-adres, IPX Extern netwerknummer, IPX Print Server.
Eigenschappen van afdrukapparaat	Omvat geïnstalleerde componenten, componentbeschrijvingen, ondersteunde functies/diensten, afdruksnelheid, kleurondersteuning, afwerkingsopties, duplexondersteuning, markeringstechnologie, harde schijf, RAM, taalondersteuning, door de gebruiker gedefinieerde eigenschappen.
Status afdrukapparaat	Omvat algemene status, gedetailleerde waarschuwingen, lokale consoleberichten, componentstatus, gegevens gerelateerd aan herstel van de status, detectiedatum, detectiemethode/-type, up-time van apparaat, ondersteunde/ingeschakelde vallen.
Tellers afdrukapparaat	Omvat facturatiemeters, printgerelateerde tellers, kopieergerelateerde tellers, faxgerelateerde tellers, tellers gerelateerd aan grote opdrachten, scangerelateerde tellers, gebruiksstatistieken en doelvolume.
Toebehoren afdrukapparaat	Omvat de naam van het verbruiksartikel, het type (bijv. beeldkwaliteit, afwerking, papiermedia), niveau, capaciteit, status, grootte en gerelateerde kenmerken.
Gedetailleerde gebruiksgegevens van afdrukapparaat	Gebruiker-gebaseerde trackinggegevens van opdrachten, met inbegrip van functiekenmerken (ID, documentnaam, eigenaar, documenttype, taaktype, kleur, duplex, vereist medium, grootte, pagina 's, sets, fouten), bestemming (afdrukapparaat, model, DNS-naam, IP-adres, MAC-adres, serienummer), resultaten van het afdrukken van de taak (indieningstijd, afdruktijd van de taak, afgedrukte pagina's, afgedrukte kleur-/zwart-witpagina's, gebruikte kleurmodus, N-up), boekhoudkundige gegevens (terugvorderingscode, terugvorderingsprijs, boekhoudkundige bron), bron van de afdruktaak (werkstation, afdrukservernaam/MAC-adres, wachtrijnaam, poort, gebruikersnaam, gebruikers-ID), Xerox-beheergegevens (verzonden naar Xerox Services Manager).
Identiteit apparaatbeheer	Bevat PC-informatie van de applicatiehost, zoals DNS-naam, IP-adres, OS-naam, OS-type, PC CPU, RAM-groottes (gratis versus gebruikt), harde schijfgroottes (gratis versus gebruikt), sitenaam, app-versie, vervaldatum van app-licentie, .Net-versie, tijdzone, detectiecomponentversie, grootte hoofddatabase, grootte detectiedatabase, aantal printers/ in scope/buiten scope, kritieke services die worden uitgevoerd.
Device Manager Bedrijfsbeveiligingsmodus	Normale modus = Xerox Device Agent neemt dagelijks contact op met Xerox Services Manager. Instellingen kunnen op afstand worden gewijzigd zonder dat bezoeken ter plaatse nodig zijn, zelfs wanneer de peilingschema's zijn uitgeschakeld. Lock Down Mode = Naast printergerelateerde gegevenssynchronisatie is er geen communicatie met Xerox Services Manager en moeten de instellingen ter plaatse worden gewijzigd. Het Xerox Device Agent-apparaat en de IP-adressen van het afdrukapparaat worden gemeld aan de Xerox Services Manager.
Beleid voor printbeheer van apparaten	Omvat de naam van de pc van de eindgebruiker, de gebruikte afdrukserver, de gebruikte afdrukwachtrij, de tijdstempel van de overtreding, de documentnaam, de gebruikersnaam van de eindgebruiker, dubbelzijdige taak, de taakkleur, de totale afdrukken van de taak, de taakprijs, de ondernomen actie, de kennisgeving aan de eindgebruiker, het weergegeven bericht, de naam van het afdrukbeleid en de regel voor het afdrukbeleid.

6. Beheer op afstand van afdrukapparaten

Het door Xerox ingezet ondersteunend personeel kan de volgende acties verwerken via Device Direct of Xerox -applicatie voor apparaatbeheer.

Tabel 4 toont vergrote resolutie-inspanningen, toegestaan door de klant in een geëscaleerd ondersteuningsscenario. Toestemming van de klant om deze functies uit te voeren moet expliciet worden verkregen.

Data	Beschrijving
Uit te voeren acties op afdrukapparaten	• Apparaatstatus ophalen = de meest recente status ophalen van het afdrukapparaat • Apparaat opnieuw opstarten = een uitschakel-/opstartsequentie starten op het afdrukapparaat • Apparaat upgraden = nieuwe software/firmware installeren op het afdrukapparaat (.DLM over poort 9100) • Problemen met apparaat oplossen = pingapparaat + laatste status ophalen van afdrukapparaat • Testpagina afdrukken = een testtaak verzenden naar een afdrukapparaat om het afdrukpad te valideren (een configuratieverslag genereren) • Start Apparaatbeheer = periodieke gegevensoverdracht van afdrukapparaten naar de externe Xerox®-communicatieservers initiëren **Opmerking: Elke actie kan worden uitgeschakeld van on-demand gebruik binnen het beheerconfiguratiegedeelte van de Xerox®-applicaties voor apparaatbeheer die deze functie ondersteunen.**
Uit te voeren acties op de applicaties voor apparaatbeheer	Instellingen binnen elke applicatie voor apparaatbeheer die kan worden beheerd, zijn onder meer detectiebewerking, data-exportfrequentie, SNMP-communicatiegerelateerde instellingen (opnieuw proberen, time-out, communitynamen), waarschuwingsprofielen en updatefrequentie van de software voor automatisch apparaatbeheer.
Beheer op afstand van software	Bepaalde apparaten zijn uitgerust met geautomatiseerde mogelijkheden voor softwarebeheer op afstand. Deze apparaten sturen een query naar de Xerox-omgeving om te zien of er nieuwe software-updates beschikbaar zijn voor het apparaat. Als die er zijn, is het apparaat in staat om vervolgens een verzoek voor die software-update te sturen. Het zal worden bijgewerkt op het voorgeschreven tijdstip. Als uw omgeving echter automatische software-updates verbiedt, kan de optie voor softwarebeheer op afstand alleen worden uitgeschakeld zonder onderbreking van standaard remote services.

Systeemvereisten voor applicaties voor apparaatbeheer

De minimumvereisten variëren enigszins naar gelang van het aanbod. Raadpleeg de gebruikershandleiding, veiligheidsbeoordelingsgids en/of certificeringshandleiding voor basisvereisten die specifiek zijn voor de respectieve applicaties voor apparaatbeheer.

Bij de installatie wordt een ReadMe-bestand bijgevoegd voor het behandelen van aanvullende en specifieke systeemvereisten voor de respectieve applicatie voor apparaatbeheer die wordt geïnstalleerd.

- De applicaties voor apparaatbeheer zijn compatibel met de beveiligingsfuncties die zijn ingebouwd in het besturingssysteem van Windows®. Ze vertrouwen op een service van Windows® die draait op de achtergrond onder de accountgegevens van het lokale systeem voor het inschakelen van proactieve monitoring van printers en de kenmerkenpayload van printgegevens die naar Xerox wordt verzonden. De gebruikersinterface die het afdrukgegevenskenmerk payload weergeeft, is alleen toegankelijk voor hoofdgebruikers en -beheerders met toegang tot het Windows®-besturingssysteem.

- Om een onderbreking van automatische communicatie op afstand te voorkomen, wordt aanbevolen dat de applicatie voor apparaatbeheer wordt geladen op een client die continu of tijdens de kernwerkuren is aangesloten.

- We raden aan dat hostcomputers uitgerust zijn met een ondersteund besturingssysteem van Microsoft® Corporation. De Xerox-applicaties voor apparaatbeheer kunnen echter worden uitgevoerd op Apple® OS 10.9.4 of hoger met de emulatiesoftware Parallels Desktop. De applicatie werkt niet in een Macintosh-omgeving. Zie de respectievelijke gebruikershandleidingen voor gedetailleerde ondersteuning. Er kunnen vereisten worden gevonden om te draaien op een Macintosh-besturingssysteem

- We raden aan dat hostcomputers up-to-date zijn met de nieuwste kritieke patches en servicereleases van Microsoft® Corporation.

- Het Network Transmission Control Protocol/Internet Protocol (TCP/IP) moet worden geladen en operationeel zijn.

- Beheerdersrechten zijn vereist om de software voor de applicatie voor apparaatbeheer op de clientmachine te installeren.

- Vereist SNMP-compatibele apparaten en de mogelijkheid om SNMP via het netwerk te routeren. Het is niet vereist om SNMP in te schakelen op de computer waarop Xerox®-applicaties voor apparaatbeheer worden geïnstalleerd of op andere netwerkcomputers.

- Microsoft®.NET Framework moet worden geïnstalleerd voordat de applicatie wordt geïnstalleerd.

- De applicatie mag niet worden geïnstalleerd op een pc waarop andere SNMP-applicaties of andere Xerox® -printerbeheertools zijn geïnstalleerd: ze kunnen elkaars werking van elkaar kunnen verstoren.

Databaseconfiguraties

- De applicatie installeert SQL Server Compact Edition (SQL CE) database engine en databasebestanden die printergegevens en applicatie-instellingen opslaan in de installatiemap. Er is geen database-licentie nodig voor de applicatie. Xerox® Device Agent ondersteunt ook bestaande exemplaren van SQL Server, zoals hierboven beschreven.

Niet-ondersteunde configuraties

Deze sectie beschrijft de configuraties die niet worden ondersteund.

- Installatie van de applicatie op een computer met een andere applicatie van Xerox voor apparaatbeheer, zoals Xerox Device Manager.

- Eigen Mac OS® besturingssysteemsoftware (d.w.z. Xerox Device Agent kan alleen worden uitgevoerd op het Apple Mac Platform wanneer de Parallels Emulation Software is geïnstalleerd.)

- Elke versie van besturingssystemen van UNIX®, Linux®, Windows® met Novell-client, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 en 2008 R2, Windows® Server 2003, Windows® 8 RT, besturingssystemen met Terminal Services voor applicaties en installatie op Windows-systemen met domeincontrollers.

Aangezien deze applicatie alleen is getest op VMware® Lab Manager/werkstation-omgeving, worden andere virtuele omgevingen niet ondersteund.

7. Bedrijfsprocessen en -diensten van Xerox®

De gegevens die worden ontvangen van Xerox® Office-gebaseerde afdrukapparaten, Xerox® Production-gebaseerde afdrukapparaten en Xerox-applicaties voor apparaatbeheer als onderdeel van de oplossing voor remote services, worden gebruikt door de hieronder vermelde bedrijfsprocessen van Xerox:

Tabel 5 geeft de naam en beschrijving van de bedrijfsprocessen en services die worden ondersteund als onderdeel van de Remote Services-oplossing.

Bedrijfsprocesnaam	Beschrijving
Automatische meterlezing	In het facturatieproces wordt gebruik gemaakt van meterafleesgegevens.
Automatisch aanvullen van voorraden/ Automatisch aanvullen van onderdelen	Toner wordt automatisch naar klanten verzonden op basis van de uitputtingsstatus van verbruiksartikelen die is ontvangen van afdrukapparaten. Bepaalde vervangbare componenten worden automatisch naar klanten verzonden wanneer dat nodig is voor hun afdrukapparaten. Deze opties zijn alleen beschikbaar voor klanten die kiezen voor gemeten leveringscontracten.
Onderhoudsvriendelijkheid (Maintenance Assistant)	Beheer op afstand van het apparaat biedt gedetailleerde foutinformatie die kan worden bekeken door het servicepersoneel van Xerox om indien nodig de voorbereiding voor een bezoek ter plaatse te versnellen of problemen te diagnosticeren en op te lossen.
Ondersteuning op derde niveau (Engineering/Debug)	Productondersteunend personeel kan moeilijke problemen debuggen wanneer het toegang krijgt tot gedetailleerde engineering- en debuglogboeken.
Productontwikkeling	Printerprestaties en gebruiksgegevens worden gebruikt om productverbeteringen voor toekomstige releases te identificeren.

De basisgegevens van het afdrukapparaat worden geaggregeerd, verzonden, bewaard en gearchiveerd in een ISO-27001-gecertificeerd Xerox-datacenter en worden bewaard in overeenstemming met het beleid van Xerox inzake het bewaren van bedrijfsgegevens.

De werkprocessen en werkwijzen die de softwaresystemen voor remote services ondersteunen en beschermen, zijn gebaseerd op ITIL-best practices en Xerox-informatiebeveiligingsbeleidslijnen die rechtstreeks in overeenstemming zijn met de ISO 27002-normen van de Internationale Organisatie voor Standaardisatie voor het beheer van informatiebeveiliging. Klanten kunnen er zeker van zijn dat het beheer, de bescherming en de opslag van apparaatgegevens de basisprincipes van informatiebeveiliging omvat: vertrouwelijkheid, integriteit, beschikbaarheid, authenticatie en niet-afwijzing.

8. Technologiedetails

Deze sectie bevat aanvullende technische details die doorgaans vereist zijn door IT-teams en beveiligingsmedewerkers die risico's beheren door zekerheid te verkrijgen over veilige ontwikkelingspraktijken. Een dergelijke garantie stelt hen in staat om onze afdrukapparaten en apparaatbeheerapplicaties te certificeren voor gebruik binnen de netwerkomgeving van de klant.

Softwareontwerp

Onze toewijding aan productbeveiliging van Xerox begint al vroeg in productontwikkeling, waarbij Xerox-ontwikkelaars een formele levenscyclus van beveiligingsontwikkeling volgen die beveiligingsproblemen beheert door identificatie, analyse, prioritering, codering en testen. Veel Xerox®-printapparaten zijn volgens gemeenschappelijke criteria gecertificeerd volgens ISO IEC 15408 of worden actief gecertificeerd.

Operationaliteit

Xerox Remote Services voert de volgende soorten bewerkingen uit op een netwerk. Deze bewerkingen zijn afhankelijk van de geconfigureerde implementatiemethode.

Tabel 6.

Implementa-tiemethode	Applicatie gebruikt	Gegevens-stroom op netwerk	Operationaliteit opgelegd aan een netwerk
Device Direct	Geen	Intern	Het Xerox®-afdrukapparaat probeert een web proxy server te detecteren (automatisch of naar een specifiek adres)
		Intern	Xerox®-afdrukapparaten kunnen worden geprogrammeerd om verzoeken te genereren naar een Simple Mail Transport Protocol (SMTP)-server voor het verzenden van e-mailnotificaties naar een gedefinieerde ontvangerslijst
		Extern naar netwerk	Het Xerox®-afdrukapparaat doorkruist de bedrijfsfirewall om toegang te krijgen tot het internet (HTTPS over poort 443)
		Extern naar netwerk	Het Xerox®-afdrukapparaat authenticeert met zijn certificaat naar de remote Xerox-communicatieserver voordat gegevenskenmerken worden verzonden
		Extern naar netwerk	Het Xerox®-afdrukapparaat verzendt dagelijks of op verzoek van de klant automatisch de kenmerkgegevens van het afdrukapparaat via een versleuteld kanaal (HTTPS over poort 443) naar de Xerox®-communicatieservers.
		Extern naar netwerk	Het Xerox®-afdrukapparaat vraagt de Xerox®-communicatieservers automatisch via een versleuteld kanaal (HTTPS over poort 443) elke dag op een specifiek tijdstip om een lijst met uit te voeren acties (bijv. nu factureringsgegevens verzenden, service toevoegen, enz.)
		Extern naar netwerk	Eenrichtingsverkeer van Xerox®-afdrukapparaat engineering log data via een versleuteld kanaal (HTTPS over poort 443) naar de Xerox®-communicatieserver

Implementa-tiemethode	Applicatie gebruikt	Gegevens-stroom op netwerk	Operationaliteit opgelegd aan een netwerk
Device Direct	Geen	Uitgaand, geïnitieerd door apparaat om laatste software op te halen	Apparaat stuurt query naar externe softwarebeheerserver om te controleren op software-/beveiligingsupdates. Als de klantomgeving echter automatische software-updates verbiedt, kan de optie voor remote softwarebeheer alleen worden uitgeschakeld zonder onderbreking van standaard remote services.
Applicaties voor apparaat-beheer	Centre Ware® Web	Intern	Elke app detecteert een web proxy server (automatisch of naar een specifiek adres)
		Intern	Elke app haalt afdrukapparaatmogelijkheden op in de hele vloot via SNMP
		Intern	Elke app haalt de configuratie van het afdrukapparaat binnen de vloot op via SNMP
		Intern	Elke app haalt afdrukapparaatstatus op in de hele vloot via SNMP
		Intern	Elke app haalt verbuiksgoederen op in de hele vloot via SNMP
		Intern	Elke app kan een afdrukapparaat opnieuw opstarten via SNMP of via de webinterface van het afdrukapparaat
		Intern	Elke app kan een testpagina indienen bij een specifiek afdrukapparaat
		Intern	Elke app kan de webpagina van een afdrukapparaat starten
		Extern **(alleen uitgaand)**	Elke app doorloopt de bedrijfsfirewall om toegang te krijgen tot het internet (HTTPS over poort 443)
		Extern (**alleen uitgaand)**	Elke app authenticeert met zijn certificaat naar de externe Xerox-communicatieserver voordat gegevensattributen worden verzonden
		Extern **(alleen uitgaand)**	Elke app verzendt automatisch de attribuutgegevens van het afdrukapparaat via een versleuteld kanaal (HTTPS over poort 443) naar de Xerox®-communicatieservers op een specifiek tijdstip elke dag
		Extern **(alleen uitgaand)**	Elke app vraagt elke dag automatisch de Xerox®-communicatieservers via een versleuteld kanaal (HTTPS over poort 443) op een specifiek tijdstip om een lijst met uit te voeren acties
		Intern	Elke Xerox Device Agent-app detecteert een web proxy server (automatisch of naar een specifiek adres)
		Intern	Elke Xerox Device Agent-app haalt de mogelijkheden van afdrukapparaten op in de hele vloot via SNMP
		Intern	Elke Xerox® Device Agent-app haalt de configuratie van het afdrukapparaat over de hele vloot op via SNMP
		Intern	Elke Xerox Device Agent-app haalt de status van afdrukapparaten op in de hele vloot via SNMP

Implementatiemethode	Applicatie gebruikt	Gegevensstroom op netwerk	Operationaliteit opgelegd aan een netwerk
Applicaties voor apparaatbeheer	Xerox	Intern	Elke Xerox Device Agent-app haalt de verbruiksgegevens van afdrukapparaten op in de hele vloot via SNMP
		Intern	Elke Xerox Device Agent-app kan verzoeken dat het apparaat een configuratieverslag afdrukt
		Intern	Elke Xerox Device Agent-app kan de webpagina van een afdrukapparaat starten
		Intern	Elke Xerox Device Agent-app kan software voor afdrukapparaten upgraden via het indienen van afdruktaken. (. DLM-bestand over poort 9100)
		Extern (**alleen uitgaand)**	Elke Xerox Device Agent-app doorkruist de bedrijfsfirewall om toegang te krijgen tot het internet (HTTPS over poort 443)
		Extern (**alleen uitgaand)**	Elke app authenticeert met zijn certificaat naar de externe Xerox-communicatieserver voordat gegevensattributen worden verzonden
		Extern **(alleen uitgaand)**	Elke Xerox Device Agent-app verzendt automatisch de attribuutgegevens van het afdrukapparaat via een versleuteld kanaal (HTTPS over poort 443) naar de Xerox®-communicatieservers op een specifiek tijdstip elke dag
		Extern **(alleen uitgaand)**	Elke Xerox Device Agent-app vraagt automatisch de communicatieservers op een specifiek tijdstip elke dag om een lijst met uit te voeren acties, via een versleuteld kanaal (HTTPS over poort 443)
Applicaties voor apparaatbeheer	Xerox® Device Manager voor het monitoren van netwerkgekoppelde afdrukapparaten	Intern	Xerox Device Manager- / Xerox Device Agent-apps detecteren een web proxy server (automatisch of doorgestuurd naar een specifiek adres)
		Intern	Xerox Device Manager- / Xerox Device Agent-apps halen de mogelijkheden van afdrukapparaten in de hele vloot op via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apps halen de configuratie van afdrukapparaten in de hele vloot op via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apps halen de status van afdrukapparaten in de hele vloot op via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apps halen de verbruiksgegevens van afdrukapparaten in de hele vloot op via SNMP
		Intern	Xerox Device Manager- / Xerox Device Agent-apps kunnen verzoeken dat het apparaat een configuratieverslag afdrukt
		Intern	Xerox Device Manager- / Xerox Device Agent-apps kunnen de webpagina van een afdrukapparaat starten
		Intern	Xerox Device Manager- / Xerox Device Agent-apps kunnen software voor afdrukapparaten upgraden via het indienen van afdruktaken
		Intern	De Xerox Device Manager-app ondersteunt SNMPv3-communicatie met afdrukapparaten

Implementa-tiemethode	Applicatie gebruikt	Gegevens-stroom op netwerk	Operationaliteit opgelegd aan een netwerk
		Intern	De Xerox Device Manager-app kan wijzigingen aanbrengen in de configuratie van het afdrukapparaat via SNMP en de webinterface
		Intern	De Xerox Device Manger-app haalt op taken gebaseerde accountinglogboeken op van bepaalde Xerox® MFP 's
		Intern	De Xerox Device Manager-app beheert / handhaaft het beleid voor afdrukbeheer
		Extern **(alleen uitgaand)**	Xerox Device Manager- / Xerox Device Agent-apps doorkruisen de bedrijfsfirewall om toegang te krijgen tot het internet (HTTPS over poort 443)
		Extern (**alleen uitgaand)**	Elke app authenticeert met zijn certificaat naar de externe Xerox-communicatieserver voordat gegevensattributen worden verzonden
		Extern **(alleen uitgaand)**	Xerox Device Manager- / Xerox Device Agent-apps verzenden elke dag automatisch afdrukapparaatgegevens naar de Xerox®-communicatieservers via een versleuteld kanaal (HTTPS over poort 443) op een specifiek tijdstip
		Extern **(alleen uitgaand)**	Xerox Device Manager- / Xerox Device Agent-apps vragen de communicatieservers van Xerox automatisch via een versleuteld kanaal (HTTPS over poort 443) elke dag op een specifiek tijdstip om een lijst met uit te voeren acties op te vragen
	Applicatie voor apparaat-beheer	Extern, bidirec-tioneel	Xerox Device Manager neemt dagelijks contact op met Xerox Services Manager en stelt beheerders in staat om instellingen op afstand te wijzigen, waardoor servicegesprekken op locatie worden vermeden.

9. Veiligheidskenmerken

SIMPLE NETWORK MANAGEMENT PROTOCOL (EENVOUDIG NETWERKBEHEERPROTOCOL - SNMP) VOOR XEROX®

Het Simple Network Management Protocol (SNMP) is het meest gebruikte netwerkbeheertool voor communicatie tussen netwerkbeheersystemen en netwerkprinters. De applicaties voor apparaatbeheer gebruiken SNMP tijdens detectiebewerkingen om gedetailleerde informatie over afdrukapparaten op te halen. Xerox®-applicaties voor apparaatbeheer ondersteunen SNMP v1/v2- en v3-protocollen. Raadpleeg de respectieve certificeringsgidsen voor de Xerox®-applicaties voor apparaatbeheer voor specifieke details.

Het SNMP v3-raamwerk ondersteunt meerdere beveiligingsmodellen, die gelijktijdig kunnen bestaan binnen een SNMP-entiteit. SNMPv3 omvat strengere beveiliging door cryptografische beveiliging toe te voegen aan SNMPv2. Bovendien is SNMPv3 achterwaarts compatibel met eerdere versies en wordt het veel gebruikt in robuuste netwerken.

Xerox -applicaties voor apparaatbeheer (Centre Ware® Web / Xerox Device Manager, Xerox Device Agent) kunnen communiceren met apparaatplatforms die voldoen aan Federal Information Processing Standard FIPS 140-2 in hun implementaties van SNMPv3.

De Xerox -applicaties voor apparaatbeheer maken geen gebruik van de Windows SNMP-service of de Windows SNMP Trap-service. Indien eerder geïnstalleerd, **moeten** deze services worden uitgeschakeld op elke pc of server waarop de Xerox-applicatie voor apparaatbeheer is geïnstalleerd.

De Xerox-applicaties voor apparaatbeheer maken gebruik van een door Xerox ontwikkelde SNMP-agent die:

- een speciaal coderings-/decodeermechanisme bevat
- volledig .NET-beheerd is
- .NET runtime executable gebruikt: dit biedt verbeterde beveiliging om aanvallen op kwetsbaarheden in software zoals ongeldige handelingen van pointer, buffer overschrijdingen en gebonden controle te voorkomen.

De Xerox-applicaties voor apparaatbeheer maken gebruik van de beveiligingsfuncties die beschikbaar zijn vanaf het Windows-besturingssysteem (OS), waaronder:

- Gebruikersauthenticatie en autorisatie
- Configuratie en beheer van diensten
- Implementatie en beheer van groepsbeleid

Windows Internet Connection Firewall (ICF), waaronder:

- Instellingen voor beveiligingslogboekregistratie
- ICMP-instellingen

Xerox-applicaties voor apparaatbeheer: **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE-applicatie Microsoft® SQL Server en de **Xerox Device Manager** maken gebruik van Microsoft® SQL Server.

De Xerox-applicaties voor apparaatbeheer kunnen worden geconfigureerd om gebruik te maken van de aanvullende Microsoft® -beveiligingsfuncties, waaronder, indien van toepassing:

- Registratie van gebruikersaccounts inschakelen
- Encryptie van Domain Name System (DNS)
- Beperk de rechten van gebruikersaccounts tot toegang tot de database (d.w.z. database-eigenaarsrechten)
- Implementatie van een door de gebruiker gedefinieerde poortnummers

Een registratiesleutel van Xerox en een geldig Xerox-account zijn vereist om gegevens te verzenden naar de externe Xerox-communicatieservers.

De externe communicatie van de Xerox-applicaties voor apparaatbeheer kan worden beïnvloed door de Windows Internet Connection Firewall. (We **raden** klanten aan de Xerox-URL op de firewall van de klant (* .support.xerox.com) op de witte lijst te plaatsen en het IP-adres op te geven dat toegang heeft tot de URL.)

De Xerox-applicaties voor apparaatbeheer worden uitgevoerd als een achtergrondproces met behulp van de referenties van lokale systeemaccounts om automatisch netwerkprintapparaten te bevragen via SNMP en periodiek afdrukapparaatattributen terug te sturen naar de Xerox Communications-servers

Toegang tot de gebruikersinterface (UI) en functies van de Xerox-applicatie voor apparaatbeheer wordt beheerd via de volgende op rollen gebaseerde privileges :

- Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators en Centre Ware® Web Customers-groepen.
- Gebruikersnamen en wachtwoorden voor de applicaties doorkruisen het netwerk niet. In plaats daarvan worden toegangstoken gebruikt (door Windows® OS-ontwerp).
- De Xerox Device Manager-applicatie biedt beveiliging op basis van het besturingselement voor het indienen van afdrukken door taken te beperken op basis van kleurgebruiksbeleid, documenttype, opdrachtkosten, tijd van de dag, toegangsbeheer voor gebruikersgroepen, duplexbeleid, toegestane taakimpressies en afdrukquota.

Opmerking: Het gebruik van SNMP door een applicatie van Xerox® Remote Services vormt geen beveiligingsrisico voor de IT-omgeving van een klant, omdat al het op SNMP gebaseerde verkeer dat door deze applicaties wordt gegenereerd of verbruikt, plaatsvindt binnen het intranet van de klant, achter de firewall. De Windows SNMP-service en de Windows SNMP Trap-service zijn standaard niet ingeschakeld in het Windows-besturingssysteem.

Bedrijfsbeveiligingsmodus

De ***geplande*** synchronisatie door de Xerox Device Agent-applicatie met de beveiligde communicatieserver wordt standaard *dagelijks* ingesteld. Merk op dat de tijd van de dag kan worden ingesteld op een gekozen tijd.

Er bestaan twee bedrijfsbeveiligingsmodi: **Normaal** en **vergrendeld.**

Wanneer ingesteld op de **Normale** modus, neemt de applicatie voor apparaatbeheer dagelijks contact op met Xerox Services Manager.Instellingen kunnen worden gewijzigd zonder dat bezoeken ter plaatse nodig zijn, zelfs wanneer de peilingschema's zijn uitgeschakeld. ***(Aanbevolen modus***).

In de **vergrendelde** modus is er, naast printergerelateerde datasynchronisatie, geen communicatie met de communicatieservers en moeten de instellingen ter plaatse te worden gewijzigd. Bovendien worden de Xerox Device Agent-machine en de IP-adressen van het afdrukapparaat niet gemeld aan de communicatieserver. Deze modus beperkt alle andere voordelen van externe diensten tot automatische facturering en leveringen, evenals diagnostische gegevens die worden gebruikt voor technische ondersteuning.

Opmerking: Als een Xerox Device Agent-versie het tabblad Beveiligingsmodus van de onderneming niet bevat, werkt deze in de normale modus.

10. Netwerkimpact

Richtlijnen voor bedrijfsnetwerken zullen doorgaans specifieke netwerkpoorten op routers en/of servers in- of uitschakelen. De meeste IT-afdelingen maken zich zorgen over de poorten die door de applicatie worden gebruikt voor uitgaand verkeer. Het uitschakelen van specifieke poorten kan de functionaliteit van de applicatie beïnvloeden. Raadpleeg de onderstaande tabel voor specifieke poorten die worden gebruikt door de processen van de applicatie. Als de applicatie moet scannen over meerdere netwerksegmenten of subnetten, moeten routers de protocollen toestaan die aan deze poortnummers zijn gekoppeld.

Protocollen, poorten en andere gerelateerde technologieën

Tabel 7 Identificeert de protocollen, poorten en technologieën die worden gebruikt binnen Xerox® Remote Services:.

Poortnummer	Protocol	Beschrijving van het gebruik	Gegevensstroom op het netwerk
Afhankelijk van de protocollen van de bovenste laag	**Internetprotocol (IP)**	**Onderliggend transport voor alle datacommunicatie**	**Intern + extern (alleen uitgaand)**
N.v.t.	Internet Control Message Protocol (ICMP)	Apparaatdetectie en probleemoplossing afdrukken	Intern
25	Simple Mail Transport Protocol (SMTP)	Afdrukapparaat + Externe proxy-app E-mailmeldingen	Intern
53	Domain Name Services (DNS)	Gebruikt voor DNS-gebaseerde detectie van afdrukapparaten	Intern
80	Hyper Text Transport Protocol (HTTP)	Query's op webpagina's van het afdrukapparaat + query's op webpagina's van de applicatie voor apparaatbeheer	Intern
135	Externe procedureoproep (RPC)	Apparaatdetectie afdrukken	Intern
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Industriestandaardprotocol gebruikt om netwerkafdrukapparaten te ontdekken + Status, tellers en voorraadgegevens ophalen + Configuratie van afdrukapparaat ophalen en toepassen. Standaard communitynamen = 'openbaar' (GET), 'privé' (SET)	Intern

Poortnummer	Protocol	Beschrijving van het gebruik	Gegevensstroom op het netwerk
443	Hyper Text Transport Protocol Secure (HTTPS)	Beveiligde webpagina-query's voor afdrukapparaten (indien geconfigureerd) + beveiligde webpagina-query's voor de remote proxy app (indien geconfigureerd) + Afdrukapparaatgegevensoverdracht terug naar de Xerox®-communicatieservers + print regelt communicatie terug naar Xerox® Device Manager	Intern + extern (alleen uitgaand)
515, 9100, 2000, 2105	TCP/IP LPR & Raw Port-afdruktaak indienen	Software-upgrade van afdrukapparaat + Diagnose van testpagina afdrukken	Intern

11. Best practices op het gebied van beveiliging

- Houd afdrukapparaten altijd up-to-date met de nieuwste firmware/software. Xerox houdt kwetsbaarheden nauwlettend in de gaten en voorziet klanten waar nodig proactief van beveiligingspatches en updates.
- Schakel waar mogelijk ongebruikte poorten en protocollen op afdrukapparaten uit. Dit wordt meestal gedaan op de webgebruikersinterface (UI) van kantoorafdrukapparaten en de lokale gebruikersinterface (UI) van afdrukapparaten van productieklasse.
- Gebruik de functies voor toegangsbeheer van gebruikers op afdrukapparaten, indien beschikbaar. Dit wordt meestal gedaan op de webgebruikersinterface (UI) van kantoorafdrukapparaten en de lokale gebruikersinterface (UI) van afdrukapparaten van productieklasse.
- Maak indien mogelijk gebruik van beveiligde protocollen. Dit wordt meestal gedaan op de webgebruikersinterface (UI) van kantoorgebaseerde afdrukapparaten en de lokale gebruikersinterface (UI) van productiegebaseerde afdrukapparaten.
- Schakel beveiligingsfuncties in die in het apparaat zijn ingebouwd (bijv. overschrijven van afbeeldingen, versleuteling van scangegevens, versleuteling van afdrukstroom, versleuteling van schijven, beveiligde afdruk, versleutelde .pdf, verificatie van CAC/PIV-toegang).

Ga naar Xerox.com/RemoteServices voor meer informatie over remote services@ Xerox.

Raadpleeg hun respectievelijke gidsen voor aanvullende en specifieke informatie over de beveiligingsmechanismen en -capaciteiten binnen de reeks Xerox-applicaties voor apparaatbeheer:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Xerox loopt voorop met proactieve beveiliging voor de opkomende bedreigingen van vandaag, of het nu gaat om apparaat- of contentbeveiliging. Ga naar www.xerox.com/security voor toegang tot een brede waaier aan beveiligingsinformatie, updates, bulletins, white papers, patches en meer.