Xerox® Remote Services

White Paper over Beveiliging

Versie 2.0

Global Remote Services

Xerox® Technology Information Management

Januari 2017

BR19369

Dit document is onderhevig aan periodieke wijzigingen. Wijzigingen, technische onnauwkeurigheden en typografische fouten worden in hierop volgende edities gecorrigeerd.

IS 614672/IS 514590

Documentversie: 2.0 (januari 2017).

Inhoudsopgave

Algemeen doel en doelgroep

Het document is bedoeld als richtlijn voor het gebruik van Xerox® Remote Services voor Xerox- en niet-Xerox-printers in netwerkomgevingen van de klant. Het is bedoeld om informatie te verschaffen over beveiliging en om uitleg te geven over de uitgebreide beveiligingsmaatregelen die in Xerox® Remote Services worden geïmplementeerd.

De doelgroep voor dit document bestaat onder meer uit technische leveranciers, IT-netwerkbeheerders en IT-beveiligingsdeskundigen die geïnteresseerd zijn in de mogelijkheden van Remote Services en de beveiligingsimplementatie van deze functies.

We raden u aan om het document eerst helemaal door te nemen voor het certificeren van Xerox®-producten en functies voor gebruik binnen de netwerkomgeving van de klant.

Remote Services

Informatie is een van de belangrijkste bedrijfsmiddelen in elke organisatie, en beveiliging is essentieel voor alle bedrijfsmiddelen waaronder multifunctionele afdrukapparaten (MFP's) die op het netwerk zijn aangesloten. In het hedendaagse “all-in-one” concept brengt het beheer van een groep multifunctionele afdrukapparaten en het gelijktijdig in stand houden van een acceptabel beveiligingsniveau, een aantal unieke uitdagingen met zich mee die vaak over het hoofd worden gezien. Xerox® begrijpt deze complexiteit en speelt in op de beveiligingsbehoeften van onze klanten. Het assortiment Xerox®-producten, Xerox®-systemen en Xerox® Remote Services is ontworpen voor een beveiligde integratie in de bestaande werkstromen van onze klanten, waarbij de nieuwste beveiligingstechnologieën worden ingezet.

De white paper met betrekking tot beveiliging van Xerox® Remote Services is bedoeld om de klant te helpen bij het begrijpen en implementeren van de juiste beveiligde oplossing voor externe diensten die compatibel is met hun netwerkinfrastractuur. De samenstelling van het klantnetwerk bepaalt welke wijzigingen nodig zijn voor de internet-firewall, webproxyservers of andere beveilingsgerelateerde netwerkinfrastructuur. De gekozen oplossing, apparaat en functies van Xerox® Remote Services zijn afhankelijk van het informatiebeveiligingsbeleid (IS-beleid) van de klant en bepalen welke werkmodus wordt gebruikt.

Xerox ® Remote Services is beschikbaar op bepaalde apparatuurmodellen. Hiermee kunnen afdrukapparaten op afstand onderhouden en ondersteund worden met gebruik van kenmerkgegevens over het afdrukapparaat, waaronder*: identiteit van het afdrukapparaat, eigenschappen van het afdrukapparaat, status, niveau van verbruiksartikelen en gedetailleerde diagnostische gegevens.*. De kenmerkgegevens van het afdrukapparaat worden rechtstreeks verzonden vanaf het afdrukapparaat (device direct) in de netwerkomgeving van de klant, via een hostapplicatie (apparaatbeheerapplicatie), of via een combinatie van beide methoden met behulp van het beveiligde communicatiepad van Xerox® Remote Services. Zowel Xerox®-apparaten als Xerox®Device Management-applicaties beschikken over een certificaat voor de verificatie met de Xerox® Communication Servers voordat de afdrukkenmerken verzonden kunnen worden. Transacties via Xerox® Remote Services zijn altijd afkomstig uit de klantomgeving en worden uitsluitend verzonden op basis van klantautorisaties.

De Xerox® Communication Servers in de V.S. voldoen aan de strengste beveiligingsvereisten voor informatiebeveiligingsbeheer. Xerox® Datacenters en de Xerox® Remote Services-applicatie voldoen aan de jaarlijkse verklaring omtrent attestatienormen (SSAE) nr. 16, Sarbanes-Oxley Act (SOX)-nalevingsvereisten en zijn ISO 27001:2013 gecertificeerd.

Er worden standaard geen klantbeelden van afdruk-, fax-, scan-, kopieerhandelingen of gevoelige informatie verzonden naar de Xerox® Communication Servers.

Klantfuncties

Xerox® Device Management-applicaties kunnen geëxporteerde gegevenslogs met afdrukapparaatkenmerken weergegeven voor controle- en verificatiedoeleinden voordat deze worden gecodeerd en verzonden naar de externe Xerox® Communication Servers. Raadpleeg voor meer informatie de handleiding voor de gebruiker van de respectievelijke Xerox® Device Management-applicatie.

Sommige kleine tot middelgrote kantoorafdrukapparaten zijn voorzien van een functie waarmee klanten de kenmerkgegevens van het afdrukapparaat kunnen downloaden en bekijken voordat deze worden gecodeerd en verzonden naar de externe Xerox® Communication Servers via de activeringsmethode Device Direct. Om te controleren of een bepaald afdrukapparaat deze mogelijkheid heeft, gaat u naar de Centreware Internet Services-pagina van het afdrukapparaat; tabblad Status, koppeling Smart eSolutions (of Externe diensten), en onder het tabblad Maintenance Assistant.

De oplossing Xerox® Remote Services kan worden aangepast aan het IS-beleid van de klant dat voorziet in een strikte beperking of begrenzing van bepaalde soorten afdrukapparaatkenmerken die buiten netwerk kunnen worden verzonden (bijv. kenmerken van het netwerkadres). Met de tools van Xerox® Device Management-applicaties kunnen geselecteerde velden worden uitgeschakeld zodat deze niet worden verzonden.

Klanten kunnen ook een *uitzonderingsaanvraag* doen tijdens de contractonderhandelingen voor een **'opt-out'** van de oplossing Remote Services. Met deze optie worden alle Remote Services-communicatie en externe ondersteuningsmogelijkheden voor de afdrukapparaten van de account voorkomen.

Voor geëscaleerde externe ondersteuningsactiviteiten kunnen klanten de functie Externe toegang zo nodig inschakelen, zodat ze softwarereleases van het afdrukapparaat, beveiligingspatches kunnen ontvangen en op afstand afdrukapparaatconfiguraties kunnen diagnosticeren, herstellen of wijzigen om vastgestelde storingen te kunnen oplossen. Met Externe toegang kan Xerox® geen klantdocumenten, -gegevens of andere informatie die aanwezig is op of verwerkt wordt op het afdrukapparaat of de informatiesystemen van de klant, bekijken of downloaden. De enige uitzondering hierop is als de klant met Xerox-ondersteuningspersoneel werkt aan een moeilijker probleem en vastgesteld wordt dat er meer informatie nodig is om het probleem op te lossen. In dat geval kan de klant beslissen om Xerox toegang te geven tot logbestanden die lokaal op het apparaat zijn opgeslagen en die gevoelige gegevens bevatten.

Zakelijke IT-teams en beveiligingsmedewerkers worden daarom aangeraden om dit volledige document te lezen voor een goed begrip van de uiteenlopende toepassingen, vereisten en functies van Xerox® Remote Services en hoe deze aansluiten op het IS-beleid van onze klanten.

Voor extra hulpbronnen over beveiliging van Xerox®-productgegevens, industriële partnerschappen en certificeringen kunt u terecht op http://www.xerox.com/security.

Implementatiemodellen

Klanten kunnen kiezen uit de volgende implementatiemodellen van Xerox ® Remote Services, die allemaal evenveel beveiliging beiden:

- **Het Device Direct-model** - Met Device Direct kunnen afdrukapparaten rechtstreeks communiceren met de externe Xerox® Communication Servers via het internet door de firewall van de klant heen.

- **Het Device Manager-applicatiemodel** - Er kan een Xerox® Device Management-applicatie (d.w.z. Device Manager) worden geïmplementeerd op het netwerk van de klant, om een subset gegevenskenmerken van afdrukapparaten te verzamelen. Er worden meerdere afdrukapparaatkenmerken verzameld en vervolgens beveiligd verzonden naar de externe Xerox® Communication Servers.

- **Het combinatie**model – implementatie van zowel Device Direct als Device Manager-applicatiemodellen.

Alle implementatiemodellen voor Xerox ® Remote Services maken gebruik van webgebaseerde protocollen en poorten volgens de industrienorm. Hiermee wordt een beveiligd, gecodeerd kanaal gemaakt voor het extern verzenden van afdrukapparaatkenmerken naar Xerox® Communication Servers die zich in redundante, beveiligde datacenters van Xerox® bevinden.

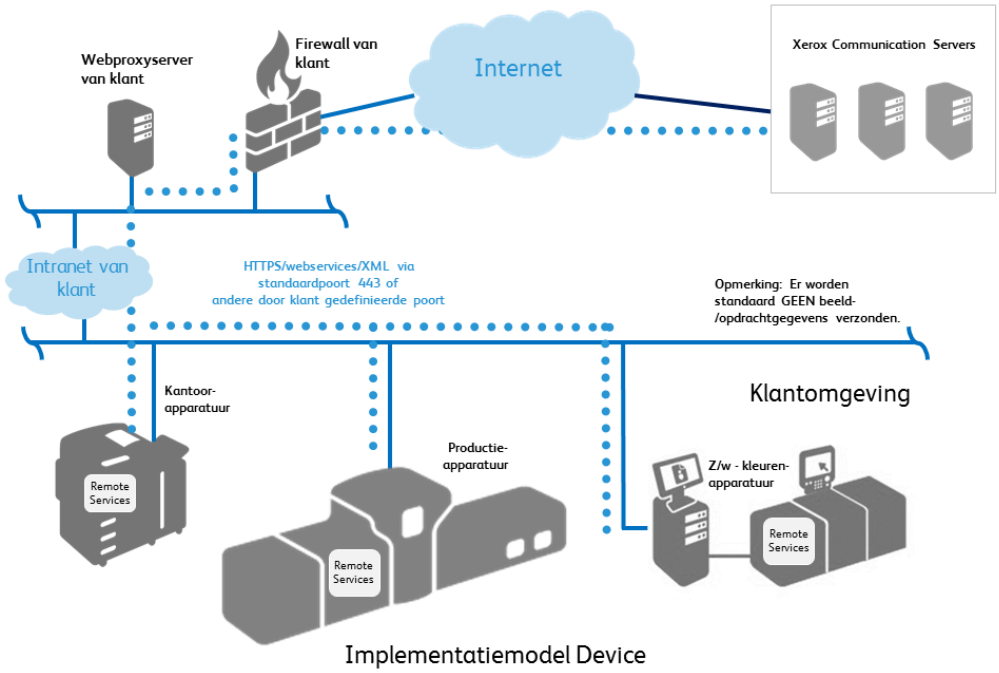
Het gekozen implementatiemodel is afhankelijk van het IS-klantbeleid en regels voor de verwerking van verzonden afdrukapparaatkenmerken en het soort afdrukoplossingen en -apparaten die zijn aangeschaft bij Xerox® (basis- of beheerde afdrukfuncties).

Implementatiemodel Device Direct

De module Remote Services die in Xerox®-apparaten is ingebouwd, maakt gebruikt van een beveiligde Transport Layer Security (TLS) 1.2-verbinding via een standaardpoort 443 voor externe communicatie met de externe Xerox® Communication Servers.

- Alle communicatie met de externe Xerox® Communication Servers wordt rechtstreeks geïnitieerd door de afdrukapparaten in de klantomgeving. Om de communicatie mogelijk te maken, zijn standaard firewallconfiguraties op de locatie nodig.
- Er moet een geldige URL voor de externe Xerox® Communication Servers worden gebruikt.
- De Xerox® Communication Servers bevinden zich achter een beveiligde firewall en zijn niet toegankelijk van het internet.

Figuur 1



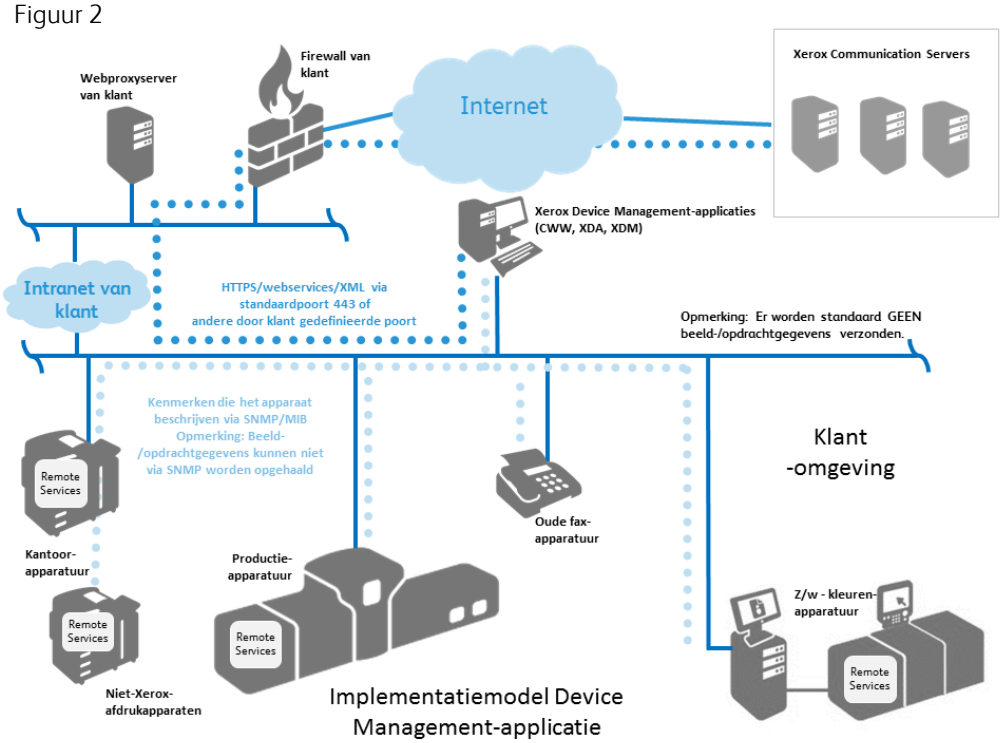
Implementatiemodel Device Direct

Implementatiemodel Device Management-applicatie

De Device Management-applicaties (d.w.z. **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition, en Xerox® Device Manager)** maken ook gebruik van een beveiligde, gecodeerde Transport Layer Security (TLS) 1.2-verbinding via de standaardpoort 443 voor externe communicatie met de externe Xerox® Communication Servers. Aanvullende functies worden gebruikt om de beveiliging van dit kanaal te verbeteren, en worden ingesteld tijdens de eerste installatie van de Device Management-applicaties. Deze bestaan onder meer uit:

- Alle communicatie met de externe Xerox® Communication Servers wordt geïnitieerd door de Device Management-applicatie in de klantomgeving. Om de communicatie mogelijk te maken, zijn standaard firewallconfiguraties op de locatie nodig.
- Er moet een geldige URL voor de externe Xerox® Communication Servers worden gebruikt.
- De Xerox® Communication Servers bevinden zich achter een beveiligde firewall en zijn niet toegankelijk van het internet.
- Er moet een geldige account-ID of locatie-ID en een registratiesleutel voor de Xerox® Communication Server worden gebruikt voor toegang tot bepaalde services van de Xerox® Communication Servers.
- De Device Management-applicatie in de klantomgeving vraagt om registratie op de externe Xerox® Communication Servers met behulp van de juiste aanmeldgegevens voor certificaatverificatie.
- De externe Xerox® Communication Servers valideren de opgegeven aanmeldgegevens en accepteren het verzoek.
- De Device Management-applicatie verifieert de externe Xerox® Communication Servers en activeert de service.

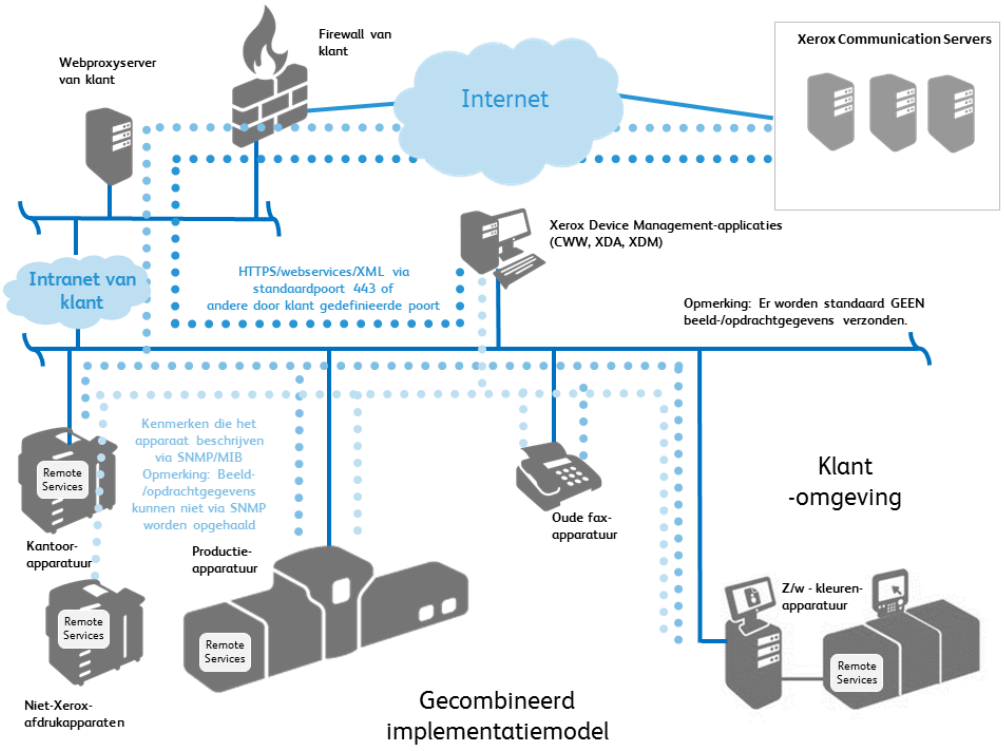
Figuur 2



Gecombineerd implementatiemodel

De gecombineerde implementatie wordt gebruikt als een klant verschillende soorten Xerox-onderhoudsovereenkomsten voor zijn afdrukapparaten aanschaft. Wanneer er in eerste instantie een Xerox®-afdrukapparaat op een netwerk wordt geïnstalleerd, is het standaardgedrag van Xerox® Remote Services dat het afdrukapparaat automatisch probeert een rechtstreekse verbinding tot stand te brengen met de Xerox® Communication Servers.

Figuur 3



Gegevensverzending en nettolading

Gegevensbronnen

De gegevenskenmerken van het afdrukapparaat worden uit de volgende bronnen verzameld voor Xerox® Remote Services:

- Xerox®-kantoornetwerkprinters
- Niet-Xerox®-netwerkprinters
- Xerox®-productieprinters
- Xerox® Device Management-applicaties

Xerox®-kantoorapparaten

Xerox®-kantoorafdrukapparaten verzenden de gegevenskenmerken van het apparaat in XML-indeling (eXtensible Markup Language) in een gecomprimeerd zipbestand. Elk bestand wordt vervolgens via een gecodeerd kanaal verzonden naar de Xerox® Communication Servers.

In tabel 1 ziet u de gegevenskenmerken van het apparaat die verzonden kunnen worden, met de bijbehorende beschrijving.

Gegevenskenmerken	Beschrijving
Afdrukapparaat-ID	Omvat model, firmwareniveau, serienummers van modules en installatiedatum.
Netwerkadres van het afdrukapparaat	Omvat het MAC-adres (Media Access Control) en subnetadres.
Eigenschappen van het afdrukapparaat	Omvat details over de configuratie van het hardwareonderdeel, details over de configuratie van de softwaremodule, ondersteunde functies/services, energiespaarstanden, etc.
Status van het afdrukapparaat	Omvat algemene status, gedetailleerde waarschuwingen, overzicht van de meest recente 40 storingen, papierstoringsgegevens, etc.
Tellers van het afdrukapparaat	Omvat factureringstellers, tellers voor afdrukken, tellers voor kopieën, tellers voor faxen, tellers voor grote opdrachten, tellers voor scannen-naar-bestemming, gebruiksstatistieken, etc.
Verbruiksartikelen voor het afdrukapparaat	Omvat naam van het verbruiksartikel, type (bijv. beeldverwerking, afwerking, papiermedia), niveau, capaciteit, status, grootte, etc.

Gegevenskenmerken	Beschrijving
Gedetailleerd afdrukapparaatgebruik	Omvat details over afdruktellers, ingeschakelde staat, details over vervangingsaantallen voor CRU's (Customer Replaceable Units, vervangbare eenheden), gedetailleerde gegevens en instanties van CRU-storingen, gebruik van de geïntegreerde OCR-functie (Optical Character Recognition, optische tekenherkenning), het aantal foutmeldingen per afdrukcyclus, aantal foutmeldingen bij gebruik van papierladen, geplaatste media, aantal foutmeldingen voor papiersoorten, aantal foutmeldingen voor papierformaten, aantal foutmeldingen voor documentlengte, het aantal sets, HFSI-gegevens, NVM-gegevens, foutmeldingen, gemarkeerd aantal pixels, gemiddelde dekking per kleur, fouten/storingen, gedetailleerde tellers voor scanopdrachten.
Engineering/debug	Omvat gedetailleerde debug-informatie, waaronder gegevens buiten de hierboven vermelde gegevensset. Deze gegevens kunnen persoonlijke informatie bevatten, zoals gebruikersnamen, e-mailadressen en opdrachtgegevens. Deze gegevens worden met expliciete toestemming van de klant verzonden en zijn alleen bestemd voor gebruik bij geëscaleerde ondersteuning.

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

Xerox®-productieapparaten

Xerox®-productieapparaten verzenden de gegevenskenmerken van het apparaat in XML-indeling (eXtensible Markup Language) in een gecomprimeerd zipbestand. Elk bestand wordt vervolgens via een gecodeerd kanaal verzonden naar de externe Xerox® Communication Servers.

In tabel 2 ziet u de gegevenskenmerken van het apparaat die verzonden kunnen worden, met de bijbehorende beschrijving.

Gegevenskenmerken	Gedetailleerde beschrijving van gegevenskenmerken
Afdrukapparaat-ID	Omvat model, firmwareniveaus van modules, serienummers van de module, installatiedatums van de module, contactgegevens van de klant, licentiegegevens en -locatie, indien beschikbaar.
Netwerkadres van het afdrukapparaat	Omvat het MAC-adres (Media Access Control) en subnetadres.
Eigenschappen van het afdrukapparaat	Omvat details over de configuratie van het hardwareonderdeel, details over de configuratie van de softwaremodule, ondersteunde functies/services, etc.
Status van het afdrukapparaat	Omvat actieve statussen, aantal opgetreden storingen, gebeurtenislogboek van DFE, overzicht van de gegevensverzendingen.
Tellers van het afdrukapparaat	Omvat factureringstellers, tellers voor afdrukken, tellers voor kopieën, tellers voor grote opdrachten, productiespecifieke tellers, tellers voor scannen-naar-bestemming op basisproductiemodellen, etc.
Verbruiksartikelen voor het afdrukapparaat	Omvat fabrikant, model, serienummer, naam, type, niveau, capaciteit, status, levensduurtellers, etc.
Gedetailleerd afdrukapparaatgebruik	Omvat HFSI-gegevens, NVM-gegevens, vervangen onderdelen, DFE-logbestanden, gedetailleerde diagnostische gegevens, oplossen van problemen.
Engineering/debug	Omvat niet-gestructureerde, gedetailleerde debug-gegevens uitsluitend bedoeld voor derdelijns-ondersteuning.
Met betrekking tot opdrachten van de klant	Met Xerox®-productieafdrukproducten kunnen opdrachtgerelateerde gegevens gereproduceerd worden ter ondersteuning van geëscaleerde ondersteuningsscenario's via gecodeerde PostScript naar Xerox. De klant kan zelf bepalen wanneer deze functie wel of niet wordt geactiveerd. Als de klant ervoor kiest om opdrachtgerelateerde gegevens (d.w.z. gecodeerde PostScript) terug te zenden naar Xerox, worden de gegevens verwerkt volgens het Xerox-IS-beleid en -normen.

Er bestaan geëscaleerde ondersteuningsscenario's met gedetailleerde debug-informatie die kan bestaan uit gegevenskenmerken die buiten de gegevensset in tabel 1-3 vallen. Deze gegevens worden verzonden met expliciete toestemming van de klant en worden verwerkt volgens het Xerox-IS-beveiligingsbeleid en -normen.

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

Xerox® Device Management-applicaties

De Xerox® Device Management-applicaties (d.w.z. Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**) en Xerox® Device Manager (**XDM**) verzenden de afdrukkenmerkgegevens in XML-indeling (eXtensible Markup Language) met behulp van een gecomprimeerd zipbestand. Het bestand wordt vervolgens gecodeerd en verzonden via gecodeerde kanalen naar de externe Xerox® Communication Servers.

In tabel 3 ziet u de gegevenskenmerken van het apparaat die via de Xerox® Device Management-applicatie verzonden kunnen worden, met de bijbehorende beschrijving.

Gegevenskenmerken	Gedetailleerde beschrijving van gegevenskenmerken
Afdrukapparaat-ID	Omvat fabrikant, model, beschrijving, firmwareniveau, serienummer, asset-tags, systeemnaam, contactpersoon, locatie, beheerstatus van het werkstation (desktop), faxtelefoonnummer en wachtrijnaam.
Netwerkadres van het afdrukapparaat	Omvat MAC-adres, IP-adres, DNS-naam, subnetmasker, standaard IP-gateway, laatst bekende IP-adres, gewijzigd IP-adres, tijdzone, IPX-adres, IPX-extern netwerknummer, IPX-afdrukserver.
Eigenschappen van het afdrukapparaat	Omvat geïnstalleerde onderdelen, beschrijvingen van de onderdelen, ondersteunde functies/services, afdruksnelheid, kleurenondersteuning, afwerkopties, dubbelzijdige ondersteuning, markeringstechnologie, harde schijf, RAM, taalondersteuning, door de gebruiker gedefinieerde eigenschappen.
Status van het afdrukapparaat	Omvat algemene status, gedetailleerde waarschuwingen, berichten op lokaal bedieningspaneel, onderdeelstatus, gegevens m.b.t. het ophalen van de status, detectiedatum, detectiemethode/-type, up-time van het apparaat, ondersteunde/ingeschakelde traps.
Tellers van het afdrukapparaat	Omvat facturerings, tellers voor afdrukken, tellers voor kopieën, tellers voor faxen, tellers voor grote opdrachten, tellers voor scannen, gebruiksstatistieken en doelvolume.
Verbruiksartikelen voor het afdrukapparaat	Omvat naam van het verbruiksartikel, type (bijv. beeldverwerking, afwerking, papiermedia), niveau, capaciteit, status, grootte, etc.
Gedetailleerd afdrukapparaatgebruik	Gebruikersgebaseerde trackinggegevens van opdrachten, waaronder opdrachtkenmerken (ID, documentnaam, eigenaar, documenttype, opdrachttype, kleur, dubbelzijdig, benodigde media, formaat, pagina's, sets, fouten), bestemming (afdrukapparaat, model, DNS-naam, IP-adres, MAC-adres, serienummer), resultaten van het afdrukken van de opdracht (verzendtijd, tijdstip waarop de opdracht is afgedrukt, afgedrukte pagina's, afgedrukte pagina's in zwart/wit of kleur, gebruikte kleurmodus, N-op-1), accountadministratiegegevens (terugbetalingscode, terugbetalingsprijs, accountadministratiebron), bron van afdrukopdracht (werkstation, naam/MAC-adres van printerserver, wachtrijnaam, poort, gebruikersnaam, gebruikers-ID), Xerox-beheergegevens (verzonden naar Xerox® Services Manager).

Gegevenskenmerken	Gedetailleerde beschrijving van gegevenskenmerken
Apparaatbeheer-ID	Omvat informatie over de applicatiehost-pc, zoals DNS-naam, IP-adres, naam besturingssysteem, soort besturingssysteem, CPU van pc, grootte van RAM (beschikbaar tegenover gebruikt), grootte van harde schijf (beschikbaar t.o.v. gebruikt), locatienaam, app-versie, vervaldatum app-licentie, .Net-versie, tijdzone, versie detectieonderdeel, grootte van hoofddatabase, grootte van detectiedatabase, aantal printers/ binnen bereik/buiten bereik, actieve essentiële services.
Device Manager - modus Bedrijfsbeveiliging	**Normale modus** = Xerox® Device Agent neemt dagelijks contact op met Xerox® Services Manager. Instellingen kunnen op afstand worden gewijzigd zonder een bezoek aan de locatie, zelfs als pollingschema's zijn uitgeschakeld. **Vergrendelde modus** = Behalve printergerelateerde gegevenssynchronisatie is er geen communicatie met Xerox® Services Manager. Instellingen moeten op de locatie worden gewijzigd. De IP-adressen van het Xerox® Device Agent-apparaat en de -printer worden doorgegeven aan Xerox® Services Manager.
Afdrukbeheerbeleid voor apparaatbeheer	Omvat pc-naam van eindgebruiker, gebruikte printerserver, gebruikte afdrukwachtrij, tijdstempel van schending, documentnaam, gebruikersnaam van eindgebruiker, opdracht dubbelzijdig, opdrachtkleur, totaal aantal afdrukken van opdracht, prijs van opdracht, ondernomen actie, eindgebruiker gewaarschuwd, weergegeven bericht, naam afdrukbeleid, regel afdrukbeleid.

Extern beheer van afdrukapparaten

Xerox® Support-medewerkers kunnen de volgende acties verwerken via de Xerox® Device Management-applicatie. Indien toegestaan worden deze acties uitgevoerd als ondersteuning bij het verhelpen van afwijkingen en staan in **tabel 4** hieronder uiteengezet.

Gegevens	Beschrijving
Acties die op afdrukapparaten moeten worden uitgevoerd	• **Apparaatstatus ophalen** = het ophalen van de meest recente status van het afdrukapparaat • **Apparaat opnieuw starten** = het starten van een uit-/inschakelingsproces op het afdrukapparaat • **Apparaat upgraden** = het installeren van nieuwe software/firmware het op afdrukapparaat (.DLM via poort 9100) • **Problemen op het apparaat oplossen** = het apparaat pingen en het ophalen van de meest recente status van het afdrukapparaat • **Testpagina afdrukken** = een testopdracht naar een afdrukapparaat verzenden om de afdrukbaan te controleren (een configuratieoverzicht genereren) • **Apparaatbeheer starten** = beginnen met de periodieke overdracht van afdrukapparaatgegevens naar de externe Xerox® Communication Servers **Opmerking:** elke actie kan op verzoek worden uitgeschakeld in het gedeelte voor configuratie van het beheer in de Xerox® Device Management-applicaties, die deze functie ondersteunen.
Acties die op afdrukapparaten moeten worden uitgevoerd	• **Apparaat opnieuw starten** = het starten van een uit-/inschakelingsproces op het afdrukapparaat • **Testpagina afdrukken** = een testopdracht naar een afdrukapparaat verzenden om de afdrukbaan te controleren (een configuratieoverzicht genereren)
Acties die in de Device Management-applicaties moeten worden uitgevoerd	De instellingen die in elke apparaatbeheerapplicatie kunnen worden beheerd, bestaan onder meer uit herkenning, frequentie van gegevensexport, instellingen met betrekking tot SNMP-communicatie (opnieuw proberen, time-out, groepsnamen) , waarschuwingsprofielen en de frequentie voor het automatisch bijwerken van de software van apparaatbeheerapplicaties.

Systeemvereisten van apparaatbeheerapplicaties

De minimale vereisten variëren afhankelijk van de aanbiedingen.. Raadpleeg de Handleiding voor de gebruiker, de Handleiding voor beoordeling van de veiligheid en/of de Handleiding voor certificering voor basisvereisten die specifiek van toepassing zijn op de respectievelijke apparaatbeheerapplicatie. Meer informatie is beschikbaar op:
http://www.support.xerox.com/support/enus.html

Bij de installatie zit een .leesmij-bestand, waarin aanvullende en specifieke systeemvereisten staan voor de respectievelijke apparaatbeheerapplicatie die wordt geïnstalleerd.

- We raden aan om hostcomputers te gebruiken met een ondersteund besturingssysteem van Microsoft ® Corporation. De Xerox® Device Management-applicaties kunnen echter ook in een Macintosh OS-omgeving worden gebruikt als de emulatiesoftware Parellels Desktop wordt gebruikt. (momenteel kunt u de Xerox® Device Management-applicatie niet in een systeemeigen Macintosh-omgeving uitvoeren.) Raadpleeg voor meer informatie de handleidingen voor de gebruiker van de respectievelijke Xerox® Device Management-applicatie.

- We raden aan om hostcomputers te gebruiken die zijn bijgewerkt met de nieuwste essentiële patches en servicereleases van Microsoft ® Corporation.

- Het netwerk-TCP/IP (Transmission Control Protocol/Internet Protocol) moet geladen en actief zijn.

- Er is een internetverbinding nodig.

- Er zijn beheerdersrechten nodig om de software van de Device Management-applicatie te kunnen installeren op het clientapparaat.

- Er zijn SNMP-apparaten nodig, en tevens de mogelijkheid tot SNMP-routering via het netwerk. SNMP hoeft niet te worden ingeschakeld op de computer waar Xerox® Device Management-applicaties worden geïnstalleerd, of op andere netwerkcomputers.

- Voordat u de applicatie installeert, meot u Microsoft®.NET Framework 4.6 (volledige versie) installeren.

- Installeer de applicatie niet op een pc waarop andere SNMP-applicaties of andere Xerox® Device Management-tools zijn geïnstalleerd, aangezien deze elkaar werking kunnen beïnvloeden.

Niet-ondersteunde configuraties

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

- Een Unix®- of Linux®-besturingssysteem

- Microsoft ®-besturingssystemen die bijna verouderd zijn, zoals Windows NT® 4.0, Windows® Media Center, Windows® XP en Windows® Server 2000 en 2003.

- Virtuele omgevingen behalve VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Deze applicatie werkt mogelijk ook in andere virtuele omgevingen. Deze omgevingen zijn echter niet getest.

Xerox®-bedrijfsprocessen en -services

De gegevens die worden ontvangen door de Xerox® Communication Servers van Xerox®-kantoorafdrukapparaten, Xerox®-productieafdrukapparaten en Xerox® Device Management-applicaties worden gebruikt door de volgende Xerox-bedrijfsprocessen:

Naam van bedrijfsproces	Beschrijving
Automatische tellerlezingen	Er wordt automatisch een factuur gegenereerd op basis van tellergegevens die van afdrukapparaten worden ontvangen.
Automatische aanvulling van verbruiksartikelen / onderdelen	Er wordt automatisch toner naar de klant verzonden wanneer de status 'verbruiksartikel is op' wordt ontvangen van afdrukapparaten. Vervangbare onderdelen worden automatisch naar de klant verzonden wanneer deze nodig zijn voor hun afdrukapparaten. Deze opties zijn alleen beschikbaar voor klanten die ervoor kiezen om een contract af te sluiten voor levering van verbruiksartikelen op basis van meteraflezingen.
Onderhoudsmogelijkheden (Maintenance Assistant)	Het Xerox-onderhoudsperoneel kan zo nodig gedetailleerde storingsgegevens bekijken als voorbereiding op een bezoek ter plaatse of om problemen extern te testen en op te lossen.
derdelijns-ondersteuning (engineering/debug)	Productondersteuningspersoneel kan moeilijke problemen debuggen wanneer ze toegang krijgen tot gedetailleerde engineering- en debuglogbestanden.

Basisgegevens over het afdrukapparaat worden gecomprimeerd, verzonden, bewaard en gearchiveerd in een ISO-27001-gecertificeerd Xerox®-datacenter en worden bewaard in overeenstemming met het Xerox®-bedrijfsbeleid met betrekking tot gegevensverwerking en -opslag.

De werkprocessen en -methoden waarmee de Xerox® Back Office Remote Services-softwaresystemen worden ondersteund en beschermd, zijn gebaseerd op de best practices van ITIL en het Xerox-informatiebeveiligingsbeleid, dat is gebaseerd op de ISO 27001-normen. Klanten kunnen erop vertrouwen dat het beheer van gegevensintegriteit, -privacy en -bescherming zijn afgestemd op de best practices.

Technologische gegevens

In dit gedeelte vindt u aanvullende technische gegevens die doorgaans nodig zijn voor het IT-team en beveiligingsmedewerkers. Het doel is daarbij om risico's te beheren door beveiligde ontwikkelingswerkwijzen toe te passen, voor de certificering van afdrukapparaten en Device Management-applicaties voor gebruik in de netwerkomgeving van de klant.

Software-ontwerp

Onze toewijding aan de beveiliging van Xerox®-producten begint al vroeg tijdens de productontwikkeling met de best practices volgens de industrienorm voor beveiligde codering, uitgebreide tests en analyses om beveiligingsproblemen te elimineren. Xerox® maakt actief gebruik van certificeringsmethoden, zoals Common Criteria, en werkt mee aan nieuwe normen, zoals P2600 Working Group en de Security Development Lifecycle (SDLC).

Werking

Xerox® Remote Services voert de volgende soorten activiteiten op een netwerk uit:

Implementatie methode	Gebruikte applicatie	Gegevensstroom op het netwerk	Aan het netwerk opgelegde functionaliteit
Device Direct	Geen	Intern	Het Xerox®-afdrukapparaat probeert een webproxyserver te vinden (automatisch of gericht op een specifiek adres)
		Intern	Xerox®-afdrukapparaten kunnen geprogrammeerd worden voor het genereren van verzoeken aan een SMTP-server (Simple Mail Transport Protocol) voor het verzenden van een waarschuwingsbericht per e-mail aan een gedefinieerde lijst met ontvangers.
		Extern naar netwerk	Het Xerox®-afdrukapparaat doorbreekt de firewall van het bedrijf voor toegang tot het internet (HTTPS via poort 443)
		Extern naar netwerk	Het Xerox®-afdrukapparaat gebruikt diens certificaat voor verificatie op de externe Xerox Communication Server voordat gegevenskenmerken worden verzonden.
		Extern naar netwerk	Het Xerox®-afdrukapparaat verzendt automatisch kenmerkgegevens van het afdrukapparaat via een gecodeerd kanaal (HTTPS via poort 443) naar de Xerox® Communication Servers op een vast dagelijks tijdstip of op verzoek van de klant.

Implementatie methode	Gebruikte applicatie	Gegevensstroom op het netwerk	Aan het netwerk opgelegde functionaliteit
		Extern naar netwerk	Het Xerox®-afdrukapparaat stuurt elke dag op een specifiek tijdstip automatisch een verzoek naar de Xerox® Communication Servers via een gecodeerd kanaal (HTTPS via poort 443) om een lijst met activiteiten die moeten worden uitgevoerd (bijv. nu factureringsgegevens verzenden, service toevoegen, etc).
		Extern naar netwerk	Eenrichtingsverzending op aanvraag van gegevens uit het engineering-logbestand voor het Xerox®-afdrukapparaat via een gecodeerd kanaal (HTTPS via poort 443) naar de Xerox® Communication Server
Device Management-applicaties	Centre Ware® Web	Intern	Elke app detecteert een webproxyserver (automatisch of gericht op een specifiek adres)
		Intern	Elk app haalt de afdrukapparaatmogelijkheden van alle apparaten op via SNMP
		Intern	Elk app haalt de afdrukapparaatconfiguratie van alle apparaten op via SNMP
		Intern	Elk app haalt de afdrukapparaatstatus van alle apparaten op via SNMP
		Intern	Elk app haalt de afdrukapparaatverbruiksartikelgegevens van alle apparaten op via SNMP
		Intern	Elke app kan een afdrukapparaat opnieuw starten via SNMP of via de web-UI van het afdrukapparaat
		Intern	Elke app kan een testpagina naar een specifiek afdrukapparaat verzenden
		Intern	Elke app kan de webpagina van een afdrukapparaat starten
		Extern **(alleen uitgaand)**	Elke app doorbreekt de firewall van het bedrijf voor toegang tot het internet (HTTPS via poort 443)
		Extern **(alleen uitgaand)**	Elke app gebruikt diens certificaat voor verificatie op de externe Xerox Communication Server voordat gegevenskenmerken worden verzonden.
		Extern **(alleen uitgaand)**	Elke app verzendt elke dag op een specifiek tijdstip automatisch kenmerkgegevens van het afdrukapapraat via een gecodeerd kanaal (HTTPS via poort 443) naar de Xerox® Communication Servers.
		Extern **(alleen uitgaand)**	Elke app stuurt elke dag op een specifieke tijdstip automatisch een verzoek naar de Xerox® Communication Servers via een gecodeerd kanaal (HTTPS via poort 443) om een lijst met activiteiten die moeten worden uitgevoerd.

Implementatie methode	Gebruikte applicatie	Gegevensstroom op het netwerk	Aan het netwerk opgelegde functionaliteit
Device Management-applicaties	Xerox® Device Agent Partner Edition voor het beheren van afdrukapparaten die op het netwerk zijn aangesloten	Intern	Elke Xerox® Device Agent-app detecteert een webproxyserver (automatisch of gericht op een specifiek adres)
		Intern	Elke Xerox® Device Agent-app haalt de afdrukapparaatmogelijkheden van alle apparaten op via SNMP
		Intern	Elke Xerox® Device Agent-app haalt de afdrukapparaatconfiguratie van alle apparaten op via SNMP
		Intern	Elke Xerox® Device Agent-app haalt de afdrukapparaatstatus van alle apparaten op via SNMP
		Intern	Elke Xerox® Device Agent-app haalt de afdrukapparaatverbruiksartikelgegevens van alle apparaten op via SNMP
		Intern	Elke Xerox® Device Agent-app kan het afdrukapparaat verzoeken om een configuratieoverzicht af te drukken
		Intern	Elke Xerox® Device Agent-app kan de webpagina van een afdrukapparaat starten
		Intern	Elke Xerox® Device Agent-app kan de software van het afdrukapparaat bijwerken via afdrukopdrachtverzending (.DLM-bestand via poort 9100)
		Extern (**alleen uitgaand)**	Elke Xerox® Device Agent-app doorbreekt de firewall van het bedrijf voor toegang tot het internet (HTTPS via poort 443)
		Extern **(alleen uitgaand)**	Elke app gebruikt diens certificaat voor verificatie op de externe Xerox Communication Server voordat gegevenskenmerken worden verzonden.
		Extern **(alleen uitgaand)**	Elke Xerox® Device Agent-app verzendt elke dag op een specifiek tijdstip automatisch kenmerkgegevens van het afdrukapparaat via een gecodeerd kanaal (HTTPS via poort 443) naar de Xerox® Communication Servers
		Extern **(alleen uitgaand)**	Elke Xerox® Device Agent-app stuurt elke dag op een specifiek tijdstip automatisch een verzoek naar de Xerox® Communication Servers via een gecodeerd kanaal (HTTPS via poort 443) om een lijst met activiteiten die moeten worden uitgevoerd
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps detecteren een webproxyserver (automatisch of gericht op een specifiek adres)

Implementatie methode	Gebruikte applicatie	Gegevensstroom op het netwerk	Aan het netwerk opgelegde functionaliteit
Device Management-applicaties	Xerox® Device Manager voor het beheren van afdrukapparaten die op het netwerk zijn aangesloten	Intern	Xerox® Device Manager / Xerox® Device Agent-apps halen de afdrukapparaatmogelijkheden van alle apparaten op via SNMP
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps halen de afdrukapparaatconfiguratie van alle apparaten op via SNMP
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps halen de afdrukapparaatstatus van alle apparaten op via SNMP
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps halen de afdrukapparaatverbruiksartikelengegevens van alle apparaten op via SNMP
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps kunnen het afdrukapparaat verzoeken om een configuratieoverzicht af te drukken
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps kunnen de webpagina van een afdrukapparaat starten
		Intern	Xerox® Device Manager / Xerox® Device Agent-apps kunnen de software van het afdrukapparaat bijwerken via afdrukopdrachtverzending
		Intern	De Xerox® Device Manager-app ondersteunt SNMPv3-communicatie met afdrukapparaten
		Intern	De Xerox® Device Agent-app kan de configuratie van het afdrukapparaat wijzigen via SNMP en de webgebruikersinterface
		Intern	De Xerox® Device Manager-app haalt de accountadministratielogbestanden per opdracht op uit bepaalde Xerox® MFP's
		Intern	De Xerox® Device Manager-app beheert/bekrachtigt dwingt afdrukbeheerbeleidsrichtlijnen
		Extern **(alleen uitgaand)**	Xerox® Device Manager / Xerox® Device Agent-apps doorbreken de firewall van het bedrijf voor toegang tot het internet (HTTPS via poort 443)
		Extern **(alleen uitgaand)**	Elke app gebruikt diens certificaat voor verificatie op de externe Xerox Communication Server voordat gegevenskenmerken worden verzonden.
		Extern **(alleen uitgaand)**	Xerox® Device Manager / Xerox® Device Agent-apps verzenden elke dag op een specifiek tijdstip automatisch afdrukapparaatgegevens naar de Xerox® Communication Servers via een gecodeerd kanaal (HTTPS via poort 443)

Implementatie methode	Gebruikte applicatie	Gegevensstroom op het netwerk	Aan het netwerk opgelegde functionaliteit
		Extern **(alleen uitgaand)**	Xerox® Device Manager / Xerox® Device Agent-apps verzenden elke dag op een specifiek tijdstip automatisch een verzoek naar de Xerox® Communication Servers via een gecodeerd kanaal (HTTPS via poort 443) om een lijst met activiteiten die moeten worden uitgevoerd

Simple Network Management Protocol (SNMP)

SNMP (Simple Network Management Protocol) is het meest gebruikte netwerkbeheerprogramma voor communicatie tussen netwerkbeheersystemen en netwerkprinters. De Device Management-applicaties gebruiken SNMP tijdens detectie om gedetailleerde afdrukapparaatinformatie op te halen van het netwerk. Xerox® Device Management-applicaties ondersteunen SNMP v1/v2- en v3-protocollen. Raadpleeg de certificeringshandleidingen van de respectievelijke Xerox® Device Managment-applicatie voor meer inzicht in de specifieke details.

Het SNMP v3-raamwerk ondersteunt meerdere beveiligingsmodellen die gelijktijdig kunnen bestaan binnen een SNMP-entiteit. SNMPv3 beschikt over strengere beveiliging door toevoeging van cryptografische beveiliging aan SNMPv2. Daarnaast is SNMPv3 is compatibel met eerdere versies en wordt veel gebruikt op robuuste netwerken.

Xerox® Device Management-applicaties (Centre Ware® Web / Xerox® Device Manager) kunnen communiceren met apparaatplatforms die FIPS 140-2-compatibel zijn bij de implementaties van SNMPv3.

De Xerox® Device Management-applicaties maken geen gebruik van de Windows SNMP-service of de Windows SNMP Trap-service. Als deze services al zijn geïnstalleerd, **moeten** ze worden uitgeschakeld op alle pc's of servers waarop de Xerox® Device Management-applicatie wordt geïnstalleerd.

De Xerox® Device Management-applicaties gebruiken een door Xerox ontwikkelde SNMP-agent die bestaat uit:

- een speciaal coderings-/decoderingsmechanisme
- volledig .NET-beheer
- het .NET uitvoerbare runtime-bestand levert verbeterde beveiliging ter preventie van aanvallen tegen kwetsbaarheden in de software, zoals ongeldige aanwijzerbewerkingen, bufferoverloop en grenscontroles.

De Xerox® Device Management-applicaties maken gebruik van de beveiligingsfuncties die beschikbaar zijn in het Windows-besturingssysteem, waaronder:

- Gebruikersverificatie en -autorisatie
- Servicesconfiguratie en -beheer
- Implementatie en beheer van groepsbeleid

Windows-firewall voor internetverbinding (Internet Connection Firewall, ICF), waaronder:

- Instellingen voor beveiligingslogboek
- ICMP-instellingen

Xerox ® Device Management-applicaties: **Xerox® Device Agent, Xerox® Device Agent Partner Edition of Xerox® Device Manager** gebruiken de SQL CE-applicatie Microsoft® SQL Server

De Xerox® Device Management-applicatie kan zodanig worden geconfigureerd dat gebruik wordt gemaakt van de aanvullende beveiligingsfuncties van de Microsoft® SQL Server-applicatie, waaronder:

- Registratie van gebruikersaccounts
- DNS-codering (Domain Name System)
- Beperkte toegangsrechten van gebruikersaccounts voor toegang tot de database (d.w.z. rechten van de eigenaar van de database)
- Implementatie van door de gebruiker gedefinieerde poortnummers

Er is een Xerox-registratiesleutel en een geldige Xerox-account nodig om gegevens te versturen naar de externe Xerox® Communications Servers.

De Windows-firewall voor de internetverbinding heeft mogelijk gevolgen voor de externe communicatie van de Xerox® Device Management-applicaties. (We **raden klanten aan** om de Xerox-URL in de whitelist op de firewall van de klant op te nemen, en het IP-adres op te geven voor toegang tot de URL.)

De Xerox® Device Management-applicaties worden als achtergrondproces uitgevoerd met de verificatiegegevens van een lokale systeemaccount om automatisch via SNMP verzoeken te verzenden naar afdrukapparaten op het netwerk en op geregelde tijden de kenmerken van de afdrukapparaten te verzenden naar de Xerox® Communications Servers.

Toegang tot de gebruikersinterface (UI) en functies van Xerox® Device Manager (XDM) wordt geregeld via de volgende op rollen gebaseerde toegangsrechten (d.w.z. CentreWare® Web Administrators, CentreWare® Web Power Users, CentreWare® Web SQL Users, CentreWare® Web Customer Administrators en opgezette CentreWare® Web Customers-groepen).

Gebruikersnamen en toegangscodes voor applicaties kunnen niet door het netwerk heen; in plaats daarvan worden toegangstokens gebruikt (dit hoort bij het ontwerp van het Windows®-besturingssysteem).

De Xerox® Device Manager (XDM)-applicaties zorgt voor beveiliging van afdrukverzendingen op basis van afdrukbeheer door beperking van opdrachten die zijn gebaseerd op het beleid voor kleurgebruik, documenttype, opdrachtkosten, tijdstip, toegangscontrole voor gebruikersgroepen, duplexbeleid, aantal toegestane afdrukken per opdracht en afdrukquota's.

Opmerkingen: het gebruik van SNMP door een Xerox® Remote Services-applicatie vormt geen beveiligingsrisico voor de IT-omgeving van de klant, omdat alle SNMP-verkeer dat door deze applicaties wordt gegenereerd of gebruikt, plaatsvindt binnen het internet van de klant, achter de firewall. De Windows SNMP-service en de Windows SNMP Trap-service zijn niet standaard binnen het Windows-besturingssysteem ingeschakeld

Modus Bedrijfsbeveiliging

Naast geplande synchronisaties door de Xerox® Device Management-applicaties naar de Xerox® Services Manager, wordt er dagelijks standaard een synchronisatie uitgevoerd. De twee modi voor bedrijfsbeveiliging zijn de **normale** en **vergrendelde** modus.

In de **normale** modus, neemt de Device Management-applicatie dagelijks contact op met de Xerox® Services Manager als alle andere geplande synchronisaties zijn uitgeschakeld ***(aanbevolen modus***).

In de **vergrendelde** modus is er behalve printergerelateerde gegevenssynchronisatie geen communicatie met Xerox® Services Manager. Deze instelling kan alleen op de locatie worden gewijzigd. (Met ***gegevenssynchronisatie*** wordt gezorgd dat de afdrukapparaatinformatie die vanuit de Xerox® Device Management-applicatie is verzonden en de informatie die is vastgelegd in Xerox® Services Manager, hetzelfde is.)

De Xerox® Device Management-applicatie neemt standaard dagelijks contact op met Xerox® Services Manager en staat beheerders toe om instellingen op afstand te wijzigen, zodat geen servicebezoeken aan de locatie nodig zijn. We raden aan om de instelling niet te wijzigen. Als een klant het Xerox-personeel geen afdrukapparaten op afstand laat ondersteunen, kan de apparaatcommunicatie met Xerox® Services Manager worden vergrendeld, behalve voor synchronisatie van printergegevens. In de modus rapporteert de applicatie geen IP-adressen van computers of printers of locatie-instellingen aan Xerox® Services Manager. Voor het wijzigen van instellingen is een bezoek aan de locatie nodig.

Opmerking: Als het tabblad Corporation Security Mode (Modus Bedrijfsbeveiliging) in Xerox® Device Agent ontbreekt, is de normale modus in gebruik.

Protocollen, poorten en andere verwante technologieën

De volgende tabel identificeert de protocollen, poorten en technologieën die binnen Xerox® Remote Services worden gebruikt:

Poortnummer	Protocol	Beschrijving van het gebruik	Gegevensstroom op het netwerk
Afhankelijk van de protocollen in de bovenste laag	**Internet Protocol (IP)**	**Onderliggend transport voor alle gegevenscommunicaties**	**Intern + extern (alleen uitgaand)**
NA	Internet Control Message Protocol (ICMP)	Detectie van afdrukapparaten + problemen oplossen	Intern
25	Simple Mail Transport Protocol (SMTP)	Afdrukapparaat + e-mailberichten met waarschuwingen via externe proxy-app	Intern
53	Domain Name Services (DNS)	Gebruikt voor herkenning van afdrukapparaten op basis van DNS	Intern
80	Hyper Text Transport Protocol (HTTP)	Webpaginaquery's over afdrukapparaat + Device Management-applicatie	Intern
135	Remote Procedure Call (RPC)	Detectie van afdrukapparaten	Intern
137, 139	NetBIOS	Detectie van printerservers	Intern

Poortnummer	Protocol	Beschrijving van het gebruik	Gegevensstroom op het netwerk
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Standaardprotocol in de industrie, gebruikt voor herkenning van afdrukapparaten in netwerken + Ophalen van status, tellers & verbruiksartikelgegevens + Ophalen & toepassen van afdrukapparaatconfiguratie Standaard groepsnamen = 'openbaar' (GET), 'privé' (SET)	Intern
162	SNMP-traps	Standaard groepsnaam = 'SNMP_trap'	Intern
389	Lightweight Direct Access Protocol (LDAP)	Detectie van afdrukapparaten via opsomming van MS Active Directory-partities + Scanserviceconfiguratieset + Active Directory-klanten importeren + Configuraties van klantengroepen	Intern
443	Hyper Text Transport Protocol Secure (HTTPS)	Beveiligde webpaginaquery's over afdrukapparaat (indien geconfigureerd) + beveiligde webpaginaquery's over externe proxy-app (indien geconfigureerd) + Overdracht van gegevens over afdrukapparaat terug naar de Xerox® Communication Servers + afdrukbeheercommunicatie terug naar Xerox® Device Manager	Intern + extern (alleen uitgaand)
452	Netware Service Advertising Protocol (SAP)	Detectie van afdrukapparaten met behulp van Novell Server-query's via IPX	Intern
515, 9100, 2000, 2105	Verzending van afdrukopdrachten via TCP/IP LPR & Raw Port	Upgrades van de software voor het afdrukapparaat + Diagnostiek via het afdrukken van een testpagina	Intern
631	Internet Printing Protocol (IPP)	Detectie van afdrukapparaten	Intern

Best practices voor beveiliging

Zorg dat afdrukapparaten altijd volledig zijn bijgewerkt met de nieuwste firmware/software. Gebruik de webgebruikersinterface (UI) van het afdrukapparaat of de printerbeheerapplicatie van Xerox® en andere afdrukleveranciers om de firmware/software van het afdrukapparaat bij te werken.

Schakel waar mogelijk ongebruikte poorten en protocollen op afdrukapparaten uit. Dit kunt u meestal doen via de webgebruikersinterface (UI) van kantoorafdrukapparaten en de lokale gebruikersinterface (UI) van productieafdrukapparaten.

Indien beschikbaar gebruikt u functies met toegangscontrole voor gebruikers op afdrukapparaten. Dit kunt u meestal doen via de webgebruikersinterface (UI) van kantoorafdrukapparaten en de lokale gebruikersinterface (UI) van productieafdrukapparaten.

Gebruik waar mogelijk beveiligde protocollen. Dit kunt u meestal doen via de webgebruikersinterface (UI) van kantoorafdrukapparaten en de lokale gebruikersinterface (UI) van productieafdrukapparaten.

Schakel interne beveiligingsfuncties op het apparaat in (bijv. beeldoverschrijving, schijfcodering, beveiligd afdrukken, etc.)

Zorg dat de bedrijfsfirewall HTTPS-pakketten via poort 443 toelaat, in overeenstemming met het beveiligingsbeleid van het bedrijf.