Fernwartungsdienste @ Xerox

Sicherheits-Whitepaper

Version 4.0

März 2022

In regelmäßigen Abständen werden Änderungen an diesem Dokument vorgenommen. Änderungen, technische Ungenauigkeiten und Schreibfehler werden in späteren Ausgaben korrigiert.

IS 614672/IS 514590

Inhaltsverzeichnis

1. Allgemeiner Zweck und Zielgruppe

Das Whitepaper „Remote Services @Xerox Security“ soll Kunden helfen, die sichere Lösung für Remote-Services zu verstehen und einzusetzen, die am besten zu ihrem Netzwerkaufbau und ihren Richtlinien der Informationssicherheit passt. Um die sicherste Konfigurationsmethode zu gewährleisten, beachten Sie bitte, dass Änderungen an der Internet-Firewall, Web-Proxy-Servern oder anderen sicherheitsrelevanten Netzwerkinfrastrukturen des Kunden erforderlich sein können.

Zur Zielgruppe dieses Dokuments gehören technische Anbieter, Netzwerkmanager und Experten für Netzwerksicherheit, die Interesse an den Remote-Services Möglichkeiten und der Sicherheitsimplementierung dieser Funktionen haben.

Wir empfehlen, das Dokument vollständig durchzuarbeiten, um die Benutzung der Xerox® -Produkte und -Dienstleistungen in der vernetzten Umgebung eines Kunden zu zertifizieren.

2. Qualitätszusage

Wir bieten eine sichere Möglichkeit, Gerätedaten an unser ISO-zertifiziertes System für die Automatisierung gängiger Aufgaben zu senden und so einen besseren Service und letztlich eine bessere Supporterfahrung zu bieten.

- Die Ablesung des Abrechnungszählers ist automatisiert und genau.
- Das automatisierte Programm für die Auffüllung von Verbrauchsmaterialien liefert Toner entsprechend der gemeldeten Tonerfüllstände des Druckers. Es ist nicht erforderlich ist, den Bestand zu verfolgen oder die Nachbestellung zu veranlassen.
- Die gesendeten Diagnoseinformationen ermöglichen uns, den Support Ihres Gerätes zu verbessern, was oft eine schnellere Problemlösung ermöglicht.
- Bestimmte Druckermodelle können nach wichtigen Software-Updates suchen und die Updates programmgesteuert ohne Zutun des Kunden installieren.[Siehe Hinweis]
- Unsere Managed Services-Funktionen können auch Drucker von Fremdherstellern zusätzlich zu Xerox-Marken-Druckern verwalten.
- Dieser Service ermöglicht unseren Kunden eine effizientere Nutzung ihrer Zeit.

All dies geschieht unter Beachtung der Sicherheit.

Hinweis: Diese Option kann für Umgebungen deaktiviert werden, in denen Kunden eine festgelegte Softwareversion zertifizieren und Drucksoftware steuern möchten, wenn Updates erfolgen. Hierzu müssen die verbleibenden Remote-Services nicht deaktiviert werden.

3. Remote-Services

Informationen sind ein zentraler Vermögenswert, und Sicherheit ist für alle organisatorischen Vermögenswerte, einschließlich vernetzter Multifunktionsdrucker (MFPs), von größter Bedeutung. Heute ist die Verwaltung einer Flotte von Multifunktionsdruckern bei gleichzeitiger Gewährleistung eines akzeptablen Sicherheitsniveaus mit einer Reihe einzigartiger Herausforderungen verbunden, die oft übersehen werden. Wir berücksichtigen diese Komplexität und reagieren auf die Sicherheitsbedürfnisse unserer Kunden. Xerox® Products, Xerox® Systems and Remote-Services sind so konzipiert, dass sie sich sicher in die bestehenden Arbeitsabläufe unserer Kunden integrieren lassen und gleichzeitig die neuesten sicheren Technologien verwenden.

Standardmäßig werden keine Abbilddateidaten von Druck-, Fax-, Scan-, Kopieraktionen oder andere sensible Informationen an unsere Server übertragen.

Die US-basierten Xerox-Server erfüllen die strengen Sicherheitsanforderungen für das Informationssicherheitsmanagement. Unsere Rechenzentren und Remote-Service-Anwendungen halten die jährliche Erklärung zu Standards for Attestation (SSAE) No-16, Sarbanes-Oxley Act (SOX) Compliance-Anforderungen ein und sind ISO 27001:2013 zertifiziert.

4. Bereitstellungsmodelle

Kunden können zwischen den folgenden gleichermaßen sicheren Xerox® Remote Services-Bereitstellungsmodellen wählen:

- **Kombinationsmodell** –***(bevorzugtes Modell)*** Die Implementierung sowohl des Device Direct als auch des Device Management-Application Modells ist ideal, da es die robustesten Daten- und Geräteverwaltungsfunktionen bietet.

- **Device Direct Model** - Device Direct ermöglicht es Druckern, direkt über das Internet durch die Firewall des Kunden mit den Remote-Xerox® -Kommunikationsservern zu kommunizieren, um Automatic Supplies Replenishment (ASR), die automatische Zählerablesung (AMR) und die Gerätediagnose-Berichterstattung zu unterstützen. Dieses Bereitstellungsmodell stellt eine Reihe von Datenelementen im Standard-Datenpaket zur Verfügung, um Gerätefehler, Warnungen, Zähler, HFSI (High Frequency Service Items) und andere Druckerattribute einzubeziehen.
- **Device Management Application Model** - Xerox® Device Management Applications können im Netzwerk eines Kunden bereitgestellt werden, um eine Reihe von Datenattributen von Druckern zu sammeln, um auch Automatic Supplies Replenishment (ASR), Automatic Meter Reads (AMR) und Gerätediagnoseberichte zu unterstützen. Druckerattribute werden gesammelt und dann sicher an die entfernten Xerox-Server übertragen.Datenattribute von Xerox- und Nicht-Xerox-Druckern können als Teil dieses Bereitstellungsmodells kommuniziert werden.

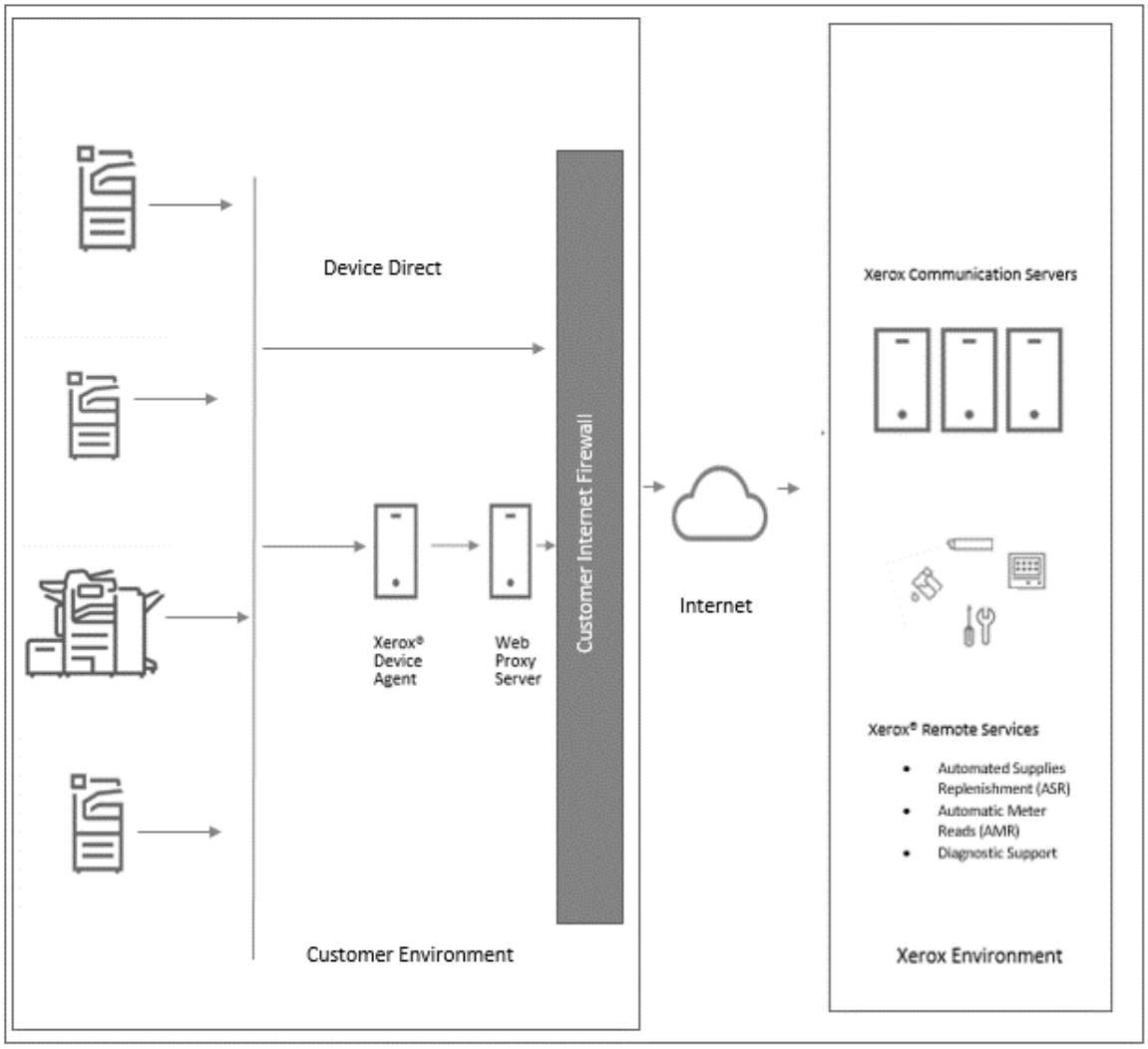
Alle Bereitstellungsmodelle für Xerox® Remote Services sind gleichermaßen sicher und nutzen die neuesten webbasierten Standardprotokolle und Ports, um einen sicheren, verschlüsselten Kanal einzurichten, wenn Druckerattribute nach extern an die entfernten Xerox-Server in unseren redundanten, gesicherten Rechenzentren übertragen werden.

Das gewählte Bereitstellungsmodell hängt von der Art der Druckdienstlösung unserer Kunden, den Richtlinien zur Informationssicherheit und den Regeln für die Handhabung der Übertragung der Datenattribute des Druckers ab.

Combination Deployment Model (bevorzugt)

Das Combination Deployment Model wird bereitgestellt, wenn ein Kunde mehrere Versionen von Xerox-Wartungsverträgen für seine Drucker kauft, um eine robustere Fernwartungs-Lösung zu erreichen. Wenn sie Xerox® Print Device Software anfänglich in einem Netzwerk installiert wird, besteht das Standardverhalten von Xerox-Fernwartungsdiensten darin, dass der Drucker automatisch versucht, nach außen über eine sichere, authentifizierte Verbindung mit unserem Kommunikationsserver zu kommunizieren.

Abbildung 1



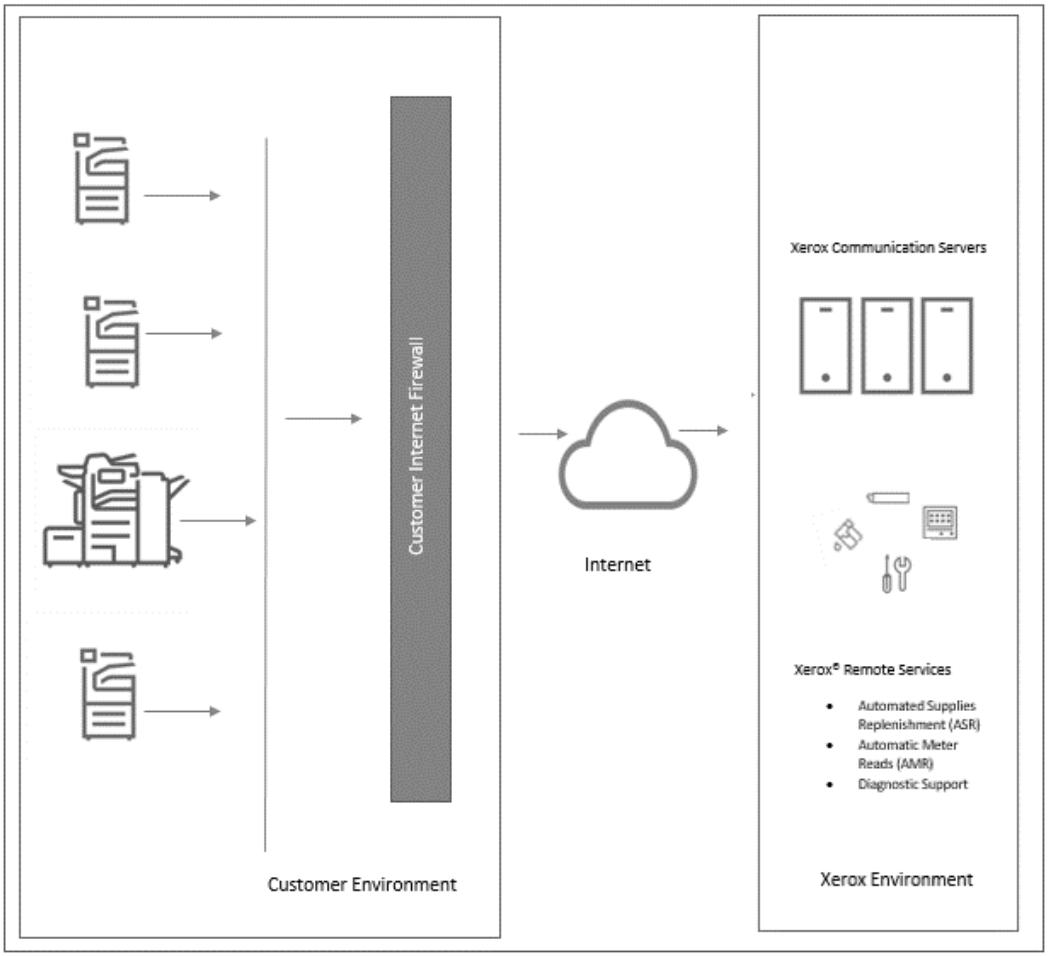
Combination Deployment Model

Device Direct Deployment Model

Remote Services-fähige Xerox® -Geräte verwenden eine Transport Layer Security (TLS) 1.2-Protokollverbindung über den sicheren Standardport 443, um über ausgehende Verbindungen mit unseren sicheren Servern zu kommunizieren.

- Drucker innerhalb der Kundenumgebung initiieren die gesamte Kommunikation mit den Kommunikationsservern. Standard-Firewall-Konfigurationen vor Ort sind erforderlich, um die Kommunikation zu ermöglichen.
- Für die Authentifizierung von Druckern an der Xerox-Infrastruktur muss eine gültige URL für die Kommunikationsserver verwendet werden (*.xerox.support.com)
- Das Gerät fragt eine Registrierung bei den Kommunikationsservern ab unter Verwendung der für die Zertifikatauthentifizierung geeigneten Anmeldedaten.
- Die Kommunikationsserver validieren die von den Druckern gelieferten Anmeldeinformationen und akzeptieren die Registrierungsanfragen.
- Die Kommunikationsserver befinden sich hinter einer sicheren Firewall und sind aus dem Internet nicht erreichbar.

Abbildung 2



Device Direct Deployment Model

Device Management Application Deployment Model

Die Device Management Applications (i.e. **Xerox Centre Ware® Web, Xerox Device Agent**, **Xerox Device Agent Lite, Xerox Device Agent Partner Edition**, **und Xerox Device Manager)** verwenden eine Transport Layer Security (TLS) 1.2-Protokollverbindung über den sicheren Standardport 443, um nach extern mit den Kommunikationsservern zu kommunizieren. Zusätzliche Funktionen werden genutzt, um die Sicherheit auf diesem Kanal zu erhöhen.
Sie werden bei der Erstinstallation der Device Management Anwendungen eingerichtet, darunter:

- Die Device Management Anwendung innerhalb der Kundenumgebung initiiert die gesamte Kommunikation mit den Kommunikationsservern. Standard-Firewall-Konfigurationen auf der Website sind erforderlich, um die Kommunikation zu ermöglichen.

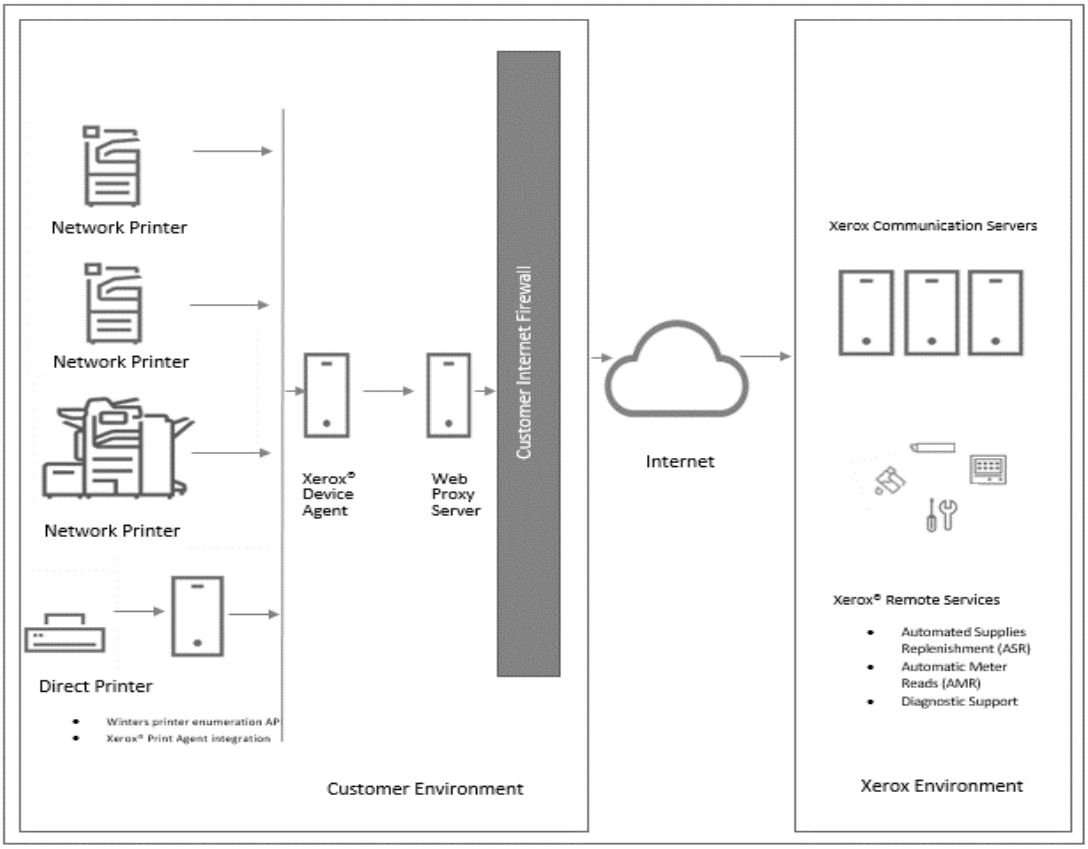
- Die Kommunikationsserver befinden sich hinter einer sicheren Firewall und sind aus dem Internet nicht erreichbar.

- Die Device Management Anwendung fragt eine Registrierung bei den Kommunikationsservern ab unter Verwendung der für die Zertifikatauthentifizierung geeigneten Anmeldedaten.

- Die Kommunikationsserver validieren die von den Druckern gelieferten Anmeldeinformationen und akzeptieren die Registrierungsanfragen.

- Die Device Management Anwendung authentifiziert die Kommunikationsserver und aktiviert den Dienst.

Abbildung 3



Device Management Application Deployment Model

5. Datenübertragung & Datenpaketnutzlasten

Datenquellen

Die Datenattribute der Drucker, die als Teil des übertragenen Datennutzlastpakets gesendet werden, stammen aus den folgenden Quellen:

- Xerox® Office-Netzwerkdrucker
- Nicht-Xerox-Netzwerkdrucker
- Xerox® Production Drucker
- Xerox® Device Management Applications

Hinweis: Nicht alle Xerox Office- und Xerox Production-Drucker sind Xerox Remote Services-fähig. Eine vollständige Liste der geeigneten Produkte finden Sie hier.Die Druckerattribute variieren je nach Produkt und Xerox® Remote Services-Bereitstellungslösung.

Xerox® Office Devices

Tabelle 1 Liste der Gerätedatenattribute, die für Remote Services-fähige Xerox® Office-Produkte übertragen werden können.

Datenattribute	Detaillierte Beschreibung der Datenattribute
Print Device Identity	Beinhaltet Modell, Modul-Firmware-levels, Modul-Seriennummern, Modul-Installationsdaten, Lizenzdaten und Standort, falls verfügbar.
Print Device Network Address	Beinhaltet die Media Access Control (MAC) Address und die Subnetzadresse.
Print Device Properties	Beinhaltet detaillierte Konfiguration der Hardwarekomponenten, detaillierte Konfiguration des Softwaremoduls, unterstützte Funktionen/Dienste usw.
Print Device Status	Beinhaltet aktive Zustände, Anzahl der Fehlerhistorien, DFE-Ereignisprotokoll, Datenübertragungshistorie
Print Device Counters	Beinhaltet Abrechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, große auftragsbezogene Zähler, produktionsspezifische Zähler, Scan-zu-Ziel-bezogene Zähler auf Low-End-Produktionsmodellen usw.
Print Device Consumables	Umfasst Hersteller, Modell, Seriennummer, Name, Typ, Füllstand, Kapazität, Status, Lebensdauerzähler usw.
Print Detailed Machine Usage	Beinhaltet HFSI-Daten, NVM-Daten, Ersatzteilaustausch, DFE-Protokolle, detaillierte Diagnosedaten, Fehlerbehebung.
Technisches/ Fehlerbehebung	Beinhaltet nicht strukturierte, Detaildaten der Fehlerbehebung, nur für die Verwendung im 3rd-Level-Support.
Customer Job-bezogen	Xerox® Production Druckprodukte bieten die Möglichkeit, auftragsbezogene Daten zur Unterstützung von eskalierten Support-Szenarien über verschlüsseltes PostScript bei Xerox abzubilden. Der Kunde kann steuern, ob er diese Funktion aktiviert oder nicht. Wenn der Kunde entscheidet, auftragsbezogene Daten (d. h. verschlüsselte PostScripts) an Xerox zurückzusenden, werden diese Daten in Übereinstimmung mit den Xerox-Richtlinien und Standards zur Informationssicherheit (IS) gehandhabt.

Unsere Drucker der Office-Klasse übertragen die Gerätedatenattribute in einem XML-Format (eXtensible Markup Language) mithilfe einer komprimierten .zip-Datei. Nach der Authentifizierung wird jede Datei dann über einen verschlüsselten Kanal an die Kommunikationsserver übertragen.

Xerox® Production Devices

Tabelle 2 Beinhaltet Gerätedatenattribute, die für Remote Services-fähige Xerox® Production Produkte übertragen werden können.

	Beschreibung
Print Device Identity	Beinhaltet Modell, Firmware-level, Seriennummern des Moduls und Installationsdatum.
Print Device Network Address	Beinhaltet die Media Access Control (MAC) Address und die Subnetzadresse.
Print Device Properties	Beinhaltet detaillierte Konfiguration der Hardwarekomponenten, detaillierte Konfiguration des Softwaremoduls, unterstützte Funktionen/Dienste, Energiesparmodi, usw.
Print Device Status	Beinhaltet den Gesamtstatus, detaillierte Warnmeldungen, den Verlauf der letzten 40 Fehler, Staudaten usw.
Print Device Counters	Beinhaltet Abrechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, Faxzähler, große auftragsbezogene Zähler, Scan-zu-Ziel-bezogene Zähler, Nutzungsstatistiken usw.
Print Device Consumables	Beinhaltet Name des Verbrauchsmaterials, Typ (z. B. Bilddruck, Finishing, Papiertyp), Füllstand, Kapazität, Status, Größe usw.
Print Detailed Machine Usage	Beinhaltet detaillierte druckbezogene Zähler, Einschaltzustände, detaillierte Austauschmengen der durch den Kunden austauschbaren Einheiten (Customer Replaceable Units, CRUs), detaillierte CRU-Fehlerdaten und Häufigkeit, Nutzung der integrierten optischen Zeichenerkennung (OCR), Verteilung der Druckauflagenhöhe, Papierfachnutzung, installierte Medien, Verteilung der Medientypen, Verteilung der Mediengröße, Verteilung der Dokumentlänge, eingestellte Nummer, HFSI-Daten, NVM-Daten, deren Verteilung, markierte Pixelanzahl, durchschnittliche Flächenabdeckung pro Farbe, Fehler/Staus, detaillierte scan-bezogene Zähler.
Technisches/ Fehlerbehebung	Enthält detaillierte Debug-Informationen, die Daten außerhalb des oben aufgeführten Datensatzes enthalten können. Diese Daten können personenbezogene Daten wie Benutzernamen, E-Mail-Adressen und Auftragsdaten enthalten. Diese Daten werden nur mit ausdrücklicher Zustimmung des Kunden gesendet und sind nur für den eskalierten Support zur Fehlerbehebung bestimmt.

Unsere Geräte der Produktionsklasse übertragen die Gerätedatenattribute in einem XML-Format (eXtensible Markup Language) mithilfe einer komprimierten .zip-Datei. Nach der Authentifizierung wird jede Datei dann über einen verschlüsselten Kanal an die Fernwartungs-Server übertragen.

Hinweis: Die Datei und der Inhalt der identifizierten Daten variieren je nach Produktmodell.

Xerox® Device Management Applications

Abhängig von der Netzwerkumgebung des Kunden und den Anforderungen an die Druckerverwaltung stehen mehrere Optionen der Device Management Application zur Verfügung. Alle sind gleichermaßen sicher und verfügen über robuste Verwaltungsfunktionen für Drucker.

Im Folgenden finden Sie eine Liste der Geräteverwaltungsanwendungen: Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition und Xerox Device Manager.

Jede Anwendung synchronisiert sich standardmäßig mindestens täglich mit den sicheren Kommunikationsservern. Um maximale Sicherheit für Ihre Daten zu gewährleisten, sind die Kommunikationsserver in einer ISO 27001-konformen Einrichtung gehostet. Bei den gesendeten Daten handelt es sich in erster Linie um druckerspezifische Abrechnungszähler, Füllstände und Druckerwarnmeldungen. Die Daten werden komprimiert, verschlüsselt und durch mehrere Mechanismen geschützt:

- Die Xerox Device Management Application initiiert den gesamten Kontakt mit den Xerox-Kommunikationsservern. Standard-Firewall-Konfigurationen in der Kundenumgebung sind erforderlich, um die Kommunikation zu ermöglichen.
- Xerox Device Management Applications benötigen einen gültigen Proxy, falls dieser für die Internetkommunikation erforderlich ist.
- Xerox-Kommunikationsserver befinden sich in der Xerox-Umgebung hinter einer sicheren Firewall und sind aus dem Internet nicht zugänglich.
- Der Zugriff auf die Benutzeroberfläche des Xerox-Kommunikationsservers erfordert eine Authentifizierung. Die Hostinformationen der Xerox Device Management Application werden in einem kundenspezifischen Konto gespeichert. Der Zugriff auf diese Kontodaten auf den Xerox-Kommunikationsservern ist auf Xerox-Kommunikationsserver-Kontomanager beschränkt.
- Die gesamte Kommunikation des Xerox-Kommunikationsservers wird protokolliert und kann angezeigt werden.
- Daten, die an Ihre vernetzten Drucker gesendet werden, bestehen, wenn aktiviert, in erster Linie aus Remote-Befehlen. Sie ermöglichen einem Account-Support-Administrator während eskalierter Support-Szenarien die Ausführung derXerox Device Management Application auf Befehlsebene anzufordern.
- Die Anforderungen beziehen sich hauptsächlich auf Firmware-Aktualisierungen, Druckerneustarts, Drucken von Testseiten und Aktualisierungen des aktuellen Gerätestatus.
- Xerox Device Management Application fragt seine Xerox-Kommunikationsserver regelmäßig nach Befehlsanforderungen ab.
- Betriebsergebnisse aus Befehlsanforderungen werden an die Xerox-Kommunikationsserver gesendet, wo sie dann überprüft werden.

Hinweis: Bei der Softwareinstallation ist eine einmalige Registrierung erforderlich. Diese Registrierungsinformationen enthalten ein Feld für den Gerätestandort und die Kontakt-E-Mail.

Die Xerox Device Management Applications **(z. B. Xerox CentreWare® Web, Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition und Xerox Device Manager**) übertragen die Druckattributdaten im eXtensible Markup Language (XML)-Format mithilfe einer komprimierten .zip-Datei. Die Datei wird dann verschlüsselt und über verschlüsselte Kanäle an die entfernten Kommunikationsserver übertragen.

Tabelle 3 Liste der Gerätedatenattribute und die Beschreibung, die über die Xerox® Device Mgmt.-App gesendet werden können.

Datenattribute	Detaillierte Beschreibung der Datenattribute
Print Device Identity	Umfasst Hersteller, Modell, Beschreibung, Firmware-levels, Seriennummer, Bestand-Schilder, Systemname, Kontakt, Standort, Verwaltungsstatus-Arbeitsplatz (Desktop), Fax-Nummer und Warteschlangenname.
Print Device Network Address	Beinhaltet MAC-Adresse, IP-Adresse, DNS-Name, Subnetzmaske, IP-Standard-Gateway, letzte bekannte IP-Adresse, geänderte IP-Adresse, Zeitzone, IPX-Adresse, IPX External Network Number, IPX Print Server.
Print Device Properties	Beinhaltet installierte Komponenten, Komponentenbeschreibungen, unterstützte Funktionen/Dienste, Druckgeschwindigkeit, Farbunterstützung, Veredelungsoptionen, Duplex-Unterstützung, Markierungstechnologie, Festplatte, RAM, Sprachunterstützung, benutzerdefinierte Eigenschaften.
Print Device Status	Beinhaltet Gesamtstatus, detaillierte Warnmeldungen, lokale Konsolenmeldungen, Komponentenstatus, Statusabruf-bezogene Daten, Erkennungsdatum, Erkennungsmethode/-typ, Betriebszeit des Gerätes, unterstützte/aktivierte Traps.
Print Device Counters	Beinhaltet Abrechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, Faxzähler, große auftragsbezogene Zähler, Scan-zu-Ziel-bezogene Zähler, Nutzungsstatistiken usw.
Print Device Consumables	Beinhaltet Name des Verbrauchsmaterials, Typ (z. B. Bilddruck, Qualität, Papiertyp), Füllstand, Kapazität, Status, Größe und ähnliche Attribute
Print Device Detailed Usage	Benutzerbasierte Auftragsverfolgungsdaten, die Auftragsmerkmale (ID, Name des Dokuments, Eigentümer, Dokumenttyp, Auftragsart, Farbe, Duplexdruck, erforderliche Medien, Größe, Seiten, Sätze, Fehler), Ziel (Drucker, Modell, DNS-Name, IP-Adresse, MAC-Adresse, Seriennummer), Ergebnisse des Druckauftrags (Übermittlungszeit, Druckzeit, gedruckte Seiten, gedruckte Farb-/B&W-Seiten, verwendeter Farbmodus, Mehrfachnutzung), Abrechnungsdaten (Rückbuchungscode, Rückbuchungspreis, Abrechnungsquelle), Quelle des Druckauftrags (Workstation, Druckservername/MAC-Adresse, Warteschlangenname, Port, Benutzername, Benutzer-ID), Xerox-Verwaltungsdaten (an Xerox Services Manager gesendet) umfassen.
Device Management Identity	Beinhaltet Informationen zum Anwendungshost-PC wie DNS-Name, IP-Adresse, Betriebssystem-Name, Betriebssystemtyp, PC-CPU, RAM-Größen (frei vs. verwendet), Festplattengrößen (frei vs. verwendet), Site-Name, App-Version, Ablaufdatum der App-Lizenz, .Net-Version, Zeitzone, Version der Discovery-Komponente, Hauptdatenbankgröße, Discovery-Datenbankgröße, Anzahl der Drucker/ im Geltungsbereich/außerhalb des Geltungsbereichs, kritische laufende Dienste.
Gerätemanager Sicherheitsmodus für Unternehmen	Normaler Modus = Xerox Device Agent kontaktiert den Xerox Services Manager, täglich. Einstellungen können aus der Ferne geändert werden, ohne dass Vor-Ort-Besuche erforderlich sind, auch wenn die Abfragezeitpläne ausgeschaltet sind. Sperrmodus = Neben der druckerbezogenen Datensynchronisation gibt es keine Kommunikation mit dem Xerox Services Manager. Die Einstellungen müssen vor Ort geändert werden. Die IP-Adressen des Xerox Device Agent-Geräts und des Druckers werden an Xerox Services Manager gemeldet.
Gerätemanagement Drucksteuerungs-richtlinie	Beinhaltet den Endbenutzer-PC-Namen, den verwendeten Druckserver, die verwendete Druckwarteschlange, den Zeitstempel des Verstoßes, den Dokumentnamen, den Benutzernamen des Endbenutzers, Duplexdruck des Auftrags, die Auftragsfarbe, die Gesamteindrücke des Auftrags, den Auftragspreis, die ergriffenen Maßnahmen, die Benachrichtigung des Endbenutzers, die angezeigte Nachricht, den Druckrichtliniennamen und die Druckrichtlinienregel.

6. Fernverwaltung von Druckgeräten

Eskaliertes Xerox Support-Personal kann die folgenden Aktionen über die Device Direct- oder Xerox Device Management Application verarbeiten.

Tabelle 4 zeigt erweiterte Lösungsbemühungen, die vom Kunden in einem eskalierten Support-Szenario zugelassen wurden. Für die Ausführung dieser Funktionen, muss die Erlaubnis des Kunden ausdrücklich eingeholt werden.

Daten	Beschreibung
Aktionen, die auf Druckern ausgeführt werden sollen	• Gerätestatus abrufen = Abrufen des neuesten Status vom Drucker • Gerät neu starten = Starten einer Abschalt-/Einschaltsequenz auf dem Drucker • Aktualisierung des Gerätes = neue Software/Firmware auf Drucker installieren (.DLM über Port 9100) • Fehlerbehebung für das Gerät = Gerät anpingen + Abrufen des neuesten Status vom Drucker • Testseite drucken = einen Testdruckauftrag an einen Drucker senden, um den Druckerpfad zu validieren (einen Konfigurationsbericht erstellen) • Verwaltung des Gerätes starten = Initiieren Sie die regelmäßigen Datenübertragungen des Druckers an die externen Xerox® Communication Server **Hinweis**: **Innerhalb der Administrationskonfiguration der Xerox® Device Management Applications wird es unterstützt, dass jede Aktion bei Bedarf deaktiviert werden kann.**
Aktionen, die in den Device Management Applications ausgeführt werden sollen	Zu den verwaltbaren Einstellungen innerhalb der einzelnen Geräteverwaltungsanwendungen gehören der Erkennungsvorgang, die Häufigkeit des Datenexports, Einstellungen für die SNMP-Kommunikation (Wiederholungsversuch, Zeitüberschreitung, Community-Namen), Warnhinweisprofile und die Aktualisierungshäufigkeit der Anwendungssoftware für die automatische Geräteverwaltung.
Remote-Software Verwaltung	Bestimmte Geräte sind mit automatisierten Funktionen der Fernverwaltungssoftware ausgestattet. Diese Geräte senden eine Abfrage an die Xerox-Umgebung, um zu sehen, ob neue Software-Updates für das Gerät verfügbar sind. Wenn dies der Fall ist, kann das Gerät eine Anfrage für dieses Software-Update senden. Zum vorgesehenen Zeitpunkt wird die Aktualisierung dann durchgeführt. Wenn Ihre Umgebung jedoch automatische Software-Updates nicht zulässt, kann die Option Fernverwaltungssoftware nur ohne Unterbrechung von Standard-Remotediensten deaktiviert werden.

Systemanforderungen für Device Management Applications

Die Mindestanforderungen variieren je nach Angebot geringfügig. Im Benutzerhandbuch, im Handbuch zur Sicherheitsbewertung und/oder im Zertifizierungshandbuch finden Sie die grundlegenden Anforderungen für die jeweiligen Geräteverwaltungsanwendungen.

Bei der Installation ist eine Liesmich-Datei enthalten, die zusätzliche und spezifische Systemanforderungen für die jeweilige zu installierende Geräteverwaltungsanwendung beschreibt.

- Die Geräteverwaltungsanwendungen sind mit den im Windows® -Betriebssystem integrierten Sicherheitsfunktionen kompatibel. Sie werden von einem Windows® -Hintergrunddienst gesteuert, der unter den Anmeldeinformationen des lokalen Systemkontos ausgeführt wird. Dies ermöglicht eine proaktive Überwachung von Druckern und der Nutzlastpakete der Druckdatenattribute, die an Xerox übertragen werden. Auf die Benutzeroberfläche, die das Nutzlastpaket der Druckdatenattribute anzeigt, können nur Poweruser und Administratoren mit Zugang zum Windows® -Betriebssystem zugreifen.

- Um eine Unterbrechung der automatischen Remote-Service-Kommunikation zu vermeiden, wird empfohlen, die Anwendung Device Management auf einen Client zu laden, der kontinuierlich oder während der Kerngeschäftszeiten mit Strom versorgt ist.

- Wir empfehlen, dass Hostcomputer ein unterstütztes Betriebssystem der Microsoft® Corporation ausführen. Die Xerox Device Management-Anwendungen können jedoch auch mit der Parallels Desktop-Emulationssoftware auf Apple® Betriebssystem (OS) 10.9.4 oder höher ausgeführt werden. Die Anwendung wird nicht in der nativen Macintosh-Umgebung ausgeführt. Detaillierten Support finden Sie in den jeweiligen Benutzerhandbüchern. Voraussetzungen für die Ausführung auf einem Macintosh-Betriebssystem können hier gefunden werden

- Wir empfehlen, dass Host-Computer mit den jüngsten kritischen Patches und Service-Releases von Microsoft® Corporation auf dem neuesten Stand sind.

- Das Network Transmission Control Protocol/Internet Protocol (TCP/IP) muss geladen und betriebsbereit sein.

- Für die Installation der Anwendungssoftware der Device Management Anwendung auf dem Clientcomputer sind Administrator-Rechte erforderlich.

- Benötigt werden SNMP-fähige Geräte und die Möglichkeit, SNMP über das Netzwerk zu routen. Es ist nicht erforderlich, SNMP weder auf dem Computer zu aktivieren, auf dem Xerox® Device Management Applications installiert wird, noch auf anderen Netzwerkcomputern.

- Microsoft®.NET Framework muss vor der Installation der Anwendung installiert sein.

- Die Anwendung sollte nicht auf einem PC installiert werden, auf dem andere SNMP-basierte Anwendungen oder andere Xerox® Print-Verwaltungstools installiert sind, da diese den Betrieb des anderen beeinträchtigen können.

Datenbankkonfigurationen

- Die Anwendung installiert SQL Server Compact Edition (SQL CE) -Datenbankmodul und -Datenbankdateien, die Druckerdaten und Anwendungseinstellungen im Installationsverzeichnis speichern. Für die Anwendung ist keine Datenbanklizensierung erforderlich. Xerox® Device Agent unterstützt auch vorhandene SQL Server, wie oben beschrieben.

Nicht unterstützte Konfigurationen

Dieser Abschnitt beschreibt die nicht unterstützten Konfigurationen.

- Installation der Anwendung auf einem Computer mit einer anderen Xerox-Geräteverwaltungsanwendung, z. B. Xerox Device Manager.

- Native Mac OS® -Betriebssystemsoftware (d. h. Xerox Device Agent kann nur auf der Apple Mac-Plattform ausgeführt werden, wenn die Parallels-Emulationssoftware installiert ist.)

- Jede Version von Unix®-Betriebssystemen, Linux®-Betriebssystemen, Windows®-Systemen, die mit Novell-Client laufen, Windows® 7, Windows® XP, Windows® Vista, Windows NT® 4.0, Windows Media® Center, Windows® 2000, Windows® Server 2008 und 2008 R2, Windows® Server 2003, Windows® 8 RT, Betriebssysteme, die mit Terminal Services für Anwendungen laufen und Installation auf Windows-Systemen, die Domänencontroller steuern.

Da diese Anwendung nur auf VMware® Lab Manager/Workstation-Umgebungen getestet wurde, werden andere virtuelle Umgebungen nicht unterstützt.

7. Xerox® Geschäftsprozess und Services

Die Daten, die von Xerox® Office-basierten Druckern, Xerox® Production-basierten Druckern und Xerox Device Management Applications als Teil der Remote-Services-Lösung erhalten wurden, werden von den nachstehend aufgeführten Xerox-Geschäftsprozessen verwendet:

Tabelle 5 listet den Namen und die Beschreibung der Geschäftsabläufe und Dienstleistungen, die als Teil der Remote Services-Lösung unterstützt werden.

Name des Geschäftsprozesses	Beschreibung
Automatische Zählerablesung	Zählerstandsdaten werden im Abrechnungsprozess verwendet.
Automatic Supplies Replenishment/Automatic Parts Replenishment	Basierend auf dem von den Druckern gemeldeten Stand der Verbrauchsmaterialien wird Toner automatisch an Kunden verschickt. Bestimmte austauschbare Komponenten werden automatisch an Kunden geliefert, sobald sie für ihre Drucker benötigt werden. Diese Optionen stehen nur für Kunden zur Verfügung, die sich vertraglich für die Fernmessung des Nachschubbedarfs entschieden haben.
Wartungsfreundlichkeit (Maintenance Assistant)	Die Fernverwaltung des Geräts liefert detaillierte Fehlerinformationen, die das Xerox-Servicepersonal bei Bedarf zur schnelleren Vorbereitung eines Kundenbesuchs einsehen kann oder um Probleme zu diagnostizieren und zu beheben.
3rd Level Support (Engineering/Debug)	Das Produkt-Support-Personal kann schwierige Probleme debuggen, wenn der Zugriff auf detaillierte Engineering- und Debug-Protokolle gewährt wird.
Produktentwicklung	Die Daten zur Druckerleistung und -nutzung werden verwendet, um Produktverbesserungen für zukünftige Versionen zu erkennen.

Die Druckerbasisdaten werden in einem ISO-27001-zertifizierten Xerox -Rechenzentrum zusammengefasst, übertragen, aufbewahrt und archiviert und gemäß den Aufbewahrungsrichtlinien für Unternehmensdaten von Xerox gespeichert.

Die Arbeitsprozesse und -praktiken, die die Fernwartungssoftware-Systeme unterstützen und schützen, basieren auf bewährten ITIL-Praktiken und den Xerox Information Security Policies, die direkt mit den Maßstäben der International Standards Organization ISO 27002 für Management-Systeme in der Informationssicherheit übereinstimmen. Kunden können sicher sein, dass die Verwaltung, der Schutz und die Speicherung von Gerätedaten die grundlegenden Prinzipien der Informationssicherheit umfassen: Vertraulichkeit, Integrität, Verfügbarkeit, Authentifizierung und unanfechtbare Gültigkeit.

8. Technologiedetails

Dieser Abschnitt enthält zusätzliche technische Details, die typischerweise von IT-Teams und in Datensicherheit erfahrene Praktiker benötigt werden, die durch zuvor erlangte Zusicherung der Entwicklungssicherheit die Risiken beherrschen. Diese Zusicherung ermöglicht es ihnen, unsere Drucker und Device Management-Anwendungen für den Einsatz in der Netzwerkumgebung des Kunden zu zertifizieren.

Software Design

Unser Engagement für die Xerox-Produktsicherheit beginnt früh in der Produktentwicklung. Xerox-Entwickler folgen einem formalen Zyklus der Sicherheitsentwicklung, der Sicherheitsprobleme durch Identifizierung, Analyse, Priorisierung, Codierung und Tests beherrscht. Viele Xerox® Print Devices sind nach Common Criteria der ISO IEC 15408 zertifiziert oder werden aktiv einer Zertifizierungsprüfung unterzogen.

Bedienbarkeit

Xerox Fernservice führt die folgenden Arten von Operationen in einem Netzwerk aus. Diese Vorgänge hängen von der konfigurierten Bereitstellungsmethode ab.

Tabelle 6.

Deployment Method	Anwendung	Datenfluss im Netzwerk	Anforderung an die Betriebsfähigkeit eines Netzwerkes
Device Direct	Keine	Intern	Xerox® Print Device versucht, einen Web Proxy Server zu erkennen (automatisch oder an eine bestimmte Adresse gerichtet)
		Intern	Xerox® Print Devices können so programmiert werden, dass Anfragen an einen SMTP-Server (Simple Mail Transport Protocol) generiert werden, um Warnmeldungen per E-Mail an eine definierte Empfängerliste zu senden
		Von extern zum Netzwerk	Xerox® Print Device geht durch die Firewall des Unternehmens in das Internet (HTTPS über Port 443)
		Von extern zum Netzwerk	Xerox® Print Device authentifiziert sich mit seinem Zertifikat beim entfernten Xerox Communication Server, bevor es Datenattribute überträgt
		Von extern zum Netzwerk	Das Xerox® Print Device überträgt die Attributdaten des Druckers automatisch über einen verschlüsselten Kanal (HTTPS über Port 443) zu einem bestimmten Zeitpunkt täglich oder auf Kundenwunsch an die Xerox® Communication Server.
		Von extern zum Netzwerk	Xerox®Print Device fragt bei Xerox® Communication Servers automatisch über einen verschlüsselten Kanal (HTTPS über Port 443) jeden Tag zu einer bestimmten Zeit eine Liste der auszuführenden Aktionen ab (z. B. jetzt Rechnungsdaten senden, Service hinzufügen usw.)

Deployment Method	Anwendung	Datenfluss im Netzwerk	Anforderung an die Betriebsfähigkeit eines Netzwerkes
		Von extern zum Netzwerk	Angeforderte Einweg-Übertragung von Xerox® Print Device technische Protokolldaten über einen verschlüsselten Kanal (HTTPS über Port 443) an den Xerox® Communication Server
Device Direct	Keine	Nach auswärts, initiiert von dev, um neueste s/w zu ziehen	Das Gerät sendet die Abfrage an den Fernverwaltungssoftware-Server, um nach Software- / Sicherheitsupdates zu suchen. Wenn die Kundenumgebung automatische Software-Updates verbietet, kann die Option Fernverwaltungsoftware nur ohne Unterbrechung von Standard-Remotediensten deaktiviert werden.
Device Management Applications	Centre Ware® Web	Intern	Jede App erkennt einen Web Proxy Server (automatisch oder an eine bestimmte Adresse gerichtet)
		Intern	Jede App ruft Druckerfunktionen über die gesamte Flotte über SNMP ab
		Intern	Jede App ruft die Druckerkonfiguration über die gesamte Flotte per SNMP ab
		Intern	Jede App ruft Druckerfunktionen über die gesamte Flotte über SNMP ab
		Intern	Jede App ruft die Druckerkonfiguration über die gesamte Flotte per SNMP ab
		Intern	Jede App kann einen Drucker über SNMP oder über die Drucker-Web-Benutzeroberfläche neu starten
		Intern	Jede App kann eine Testseite an einen bestimmten Drucker senden
		Intern	Jede App kann die Webseite eines Druckers starten
		Extern **(nur nach Extern)**	Jede App geht durch die Firewall des Unternehmens in das Internet (HTTPS über Port 443)
		Extern (**nur nach Extern)**	Jede App authentifiziert sich mit ihrem Zertifikat am entfernten Xerox Communication Server, bevor sie Datenattribute überträgt
		Extern **(nur nach Extern)**	Jede App überträgt automatisch jeden Tag zu einer bestimmten Zeit Druckerattributdaten über einen verschlüsselten Kanal (HTTPS über Port 443) an die Xerox® Communication Server
		Extern **(nur nach Extern)**	Jede App fragt die Xerox® Communication Server automatisch über einen verschlüsselten Kanal (HTTPS über Port 443) jeden Tag zu einer bestimmten Zeit nach einer Liste der auszuführenden Aktionen ab
Device Management Applications	Xerox	Intern	Jede App erkennt einen Web Proxy Server (automatisch oder an eine bestimmte Adresse gerichtet)
		Intern	Jede Xerox Device Agent-App ruft Druckerfunktionen flottenweit über SNMP ab
		Intern	Jede Xerox® Device Agent-App ruft die Druckerkonfiguration flottenweit über SNMP ab
		Intern	Jede Xerox Device Agent-App ruft Druckerfunktionen flottenweit über SNMP ab

Deployment Method	Anwendung	Datenfluss im Netzwerk	Anforderung an die Betriebsfähigkeit eines Netzwerkes
		Intern	Jede Xerox Device Agent-App ruft die Daten der Verbrauchsmaterialien der Drucker flottenweit über SNMP ab
		Intern	Jede Xerox Device Agent-App kann anfordern, dass das Gerät einen Konfigurationsbericht druckt
		Intern	Jede Xerox Device Agent-App kann die Webseite eines Druckers starten
		Intern	Jede Xerox Device Agent-App kann die Druckersoftware über die Druckauftragsübermittlung aktualisieren. (. DLM-Datei über Port 9100)
		Extern (**nur nach Extern)**	Jede Xerox Device Agent App geht durch die Firewall des Unternehmens in das Internet (HTTPS über Port 443)
		Extern (**nur nach Extern)**	Jede App authentifiziert sich mit ihrem Zertifikat am entfernten Xerox Communication Server, bevor sie Datenattribute überträgt
		Extern **(nur nach Extern)**	Jede Xerox Device Agent-App überträgt automatisch jeden Tag zu einer bestimmten Zeit Druckerattributdaten über einen verschlüsselten Kanal (HTTPS über Port 443) an die Xerox® Communication Server
		Extern **(nur nach Extern)**	Jede Xerox Device Agent App fragt die Communication Server automatisch über einen verschlüsselten Kanal (HTTPS über Port 443) jeden Tag zu einer bestimmten Zeit nach einer Liste der auszuführenden Aktionen ab
Device Management Applications	Xerox® Device Manager zur Überwa-chung von Netzwerk-druckern	Intern	Xerox Device Manager/Xerox Device Agent-Apps erkennen einen Web Proxy Server (automatisch oder an eine bestimmte Adresse gerichtet)
		Intern	Xerox Device Manager/Xerox Device Agent-Apps rufen Druckerfunktionen flottenweit über SNMP ab
		Intern	Xerox Device Manager / Xerox Device Agent-Apps rufen die Konfiguration von Druckern flottenweit über SNMP ab
		Intern	Xerox Device Manager/Xerox Device Agent-Apps rufen den Status der Druckerfunktionen flottenweit über SNMP ab
		Intern	Xerox Device Manager/Xerox Device Agent-Apps rufen die Daten der Verbrauchsmaterialien der Drucker flottenweit über SNMP ab
		Intern	Xerox Device Manager/Xerox Device Agent-Apps können einen gedruckten Konfigurationsbericht vom Gerät abrufen
		Intern	Xerox Device Manager/Xerox Device Agent-Apps können die Webseite eines Druckers starten
		Intern	Xerox Device Manager/Xerox Device Agent-Apps können die Druckersoftware über die Druckauftragsübermittlung aktualisieren
		Intern	Die Xerox Device Manager-App unterstützt SNMPv3-Kommunikation mit Druckern
		Intern	Die Xerox Device Manager-App kann Änderungen an der Druckerkonfiguration über SNMP und Web-Benutzeroberfläche vornehmen

Deployment Method	Anwendung	Datenfluss im Netzwerk	Anforderung an die Betriebsfähigkeit eines Netzwerkes
		Intern	Die Xerox Device Manger-App ruft auftragsbasierte Buchhaltungsprotokolle von bestimmten Xerox® MFPs ab
		Intern	Die Xerox Device Manager-App verwaltet/setzt Drucksteuerungsrichtlinien durch
		Extern **(nur nach Extern)**	Xerox Device Manager/Xerox Device Agent-Apps gehen durch die Firewall des Unternehmens in das Internet (HTTPS über Port 443)
		Extern (**nur nach Extern)**	Jede App authentifiziert sich mit ihrem Zertifikat am entfernten Xerox Communication Server, bevor sie Datenattribute überträgt
		External **(nur nach Extern)**	Xerox Device Manager/Xerox Device Agent-Apps übertragen täglich automatisch Druckerdaten über einen verschlüsselten Kanal (HTTPS über Port 443) zu einer bestimmten Zeit an die Xerox® Communication Server
		Extern **(nur nach Extern)**	Xerox Device Manager/Xerox Device Agent-Apps fragen die Xerox Communication Server automatisch über einen verschlüsselten Kanal (HTTPS über Port 443) jeden Tag zu einer bestimmten Zeit nach einer Liste der auszuführenden Aktionen ab
	Device Management Application	Extern, bidirektional	Xerox Device Manager kontaktiert Xerox Services Manager täglich und ermöglicht Administratoren, Einstellungen aus der Ferne zu ändern, wodurch Serviceanrufe vor Ort vermieden werden.

9. Security Features

SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) FÜR XEROX®

Das Simple Network Management Protocol (SNMP) ist das am weitesten verbreitete Netzwerkmanagement-Tool für die Kommunikation zwischen Systemen des Netzwerkmanagements und vernetzten Druckern. Die Device Management Applications verwenden SNMP während der Ermittlungsvorgänge, um detaillierte Druckerinformationen abzurufen. Xerox® Device Management Applications unterstützt SNMP v1/v2- und v3-Protokolle. Weitere Informationen finden Sie in den jeweiligen Zertifizierungsleitfäden der Xerox® Device Management Application.

Das SNMP V3 Framework unterstützt mehrere Sicherheitsmodelle, die gleichzeitig in einer SNMP-Einheit existieren können. SNMPv3 enthält eine höhere Sicherheit durch Hinzufügen von kryptographischer Sicherheit zu SNMPv2. Darüber hinaus ist SNMPv3 abwärtskompatibel zu früheren Versionen und wird häufig in robusten Netzwerken verwendet.

Xerox Device Management-Apps (Centre Ware® Web/Xerox Device Manager, Xerox Device Agent) können mit Geräteplattformen kommunizieren, die die Federal Information Processing Standard FIPS 140-2 in ihren Implementierungen von SNMPv3 erfüllen.

Die Xerox -Device Management Applications verwenden weder den Windows SNMP-Dienst noch den Windows SNMP Trap-Dienst. Wenn diese Dienste zuvor installiert wurden, **müssen** sie auf jedem PC oder Server deaktiviert werden, auf dem die Xerox Device Management Application installiert ist.

Die Xerox Device Management Applications verwenden einen von Xerox entwickelten SNMP-Agenten, der:

- einen speziellen Kodier-/Dekodiermechanismus enthält
- Ist komplett .NET-verwaltet
- Verwendet .NET Runtime Executable - dies bietet verbesserte Sicherheit, um Angriffe gegen Software-Schwachstellen wie ungültige Zeigermanipulationen, Pufferüberläufe und gebundene Überprüfung zu verhindern.

Die Xerox Device Management Applications nutzen die vom Windows-Betriebssystem (OS) verfügbaren Sicherheitsfunktionen, einschließlich:

- Benutzerauthentifizierung und -autorisierung
- Konfiguration und Verwaltung von Diensten
- Bereitstellung von Gruppenrichtlinien und Management

Windows Internet Connection Firewall (ICF), einschließlich:

- Einstellungen für die Sicherheitsprotokollierung

- ICMP-Einstellungen

Xerox Device Management Applications : **Xerox Device Agent, Xerox Device Agent Lite, Xerox Device Agent Partner Edition,** SQL CE Anwendung Microsoft® SQL Server und der **Xerox Device Manager** verwenden Microsoft® SQL Server.

Die Xerox Device Management Applications können so konfiguriert werden, dass sie die zusätzlichen Microsoft® -Sicherheitsfunktionen nutzen, die gegebenenfalls Folgendes umfassen:

- Aktivieren der Benutzerkonto-Registrierung
- Verschlüsselung des Domain Name Systems (DNS)
- Benutzerkontenberechtigungen für den Zugriff auf die Datenbank beschränken (d. h. Datenbankinhaberrechte)
- Implementierung einer benutzerdefinierten Portnummer

Ein Xerox-Registrierungsschlüssel und ein gültiges Xerox-Konto sind erforderlich, um Daten an die entfernten Xerox Communications Server zu übertragen.

Die externe Kommunikation der Xerox-Geräteverwaltungsanwendungen kann durch die Windows Internet Connection Firewall beeinträchtigt werden. (Wir**empfehlen** , dass Kunden die Xerox-URL auf der Kunden-Firewall (*.support.xerox.com) auf die Whitelist setzen und die IP-Adresse angeben, die auf die URL zugreifen kann**.**)

Die Xerox Device Management Applications laufen als Hintergrundprozess unter Verwendung von Informationen zur lokalen Systemkontenanmeldung, um automatisch Netzwerkdrucker über SNMP abzufragen und Druckerattribute periodisch an die Xerox Communications Server zurückzusenden

Der Zugriff auf die Benutzeroberflächen (UI) und Funktionen der Xerox Device Manager Application wird über die folgenden rollenbasierten Berechtigungen gesteuert:

- Centre Ware® Web Administrators, Centre Ware® Web Power Users, Centre Ware® Web SQL Users, Centre Ware® Web Customer Administrators, and Centre Ware® Web Customers Gruppen.
- Benutzernamen und Passwörter für die Anwendungen durchlaufen das Netzwerk nicht; stattdessen werden Zugriffstoken verwendet (durch Windows® OS-Design).
- Die Anwendung Xerox Device Manager bietet eine auf Druckvorlagensteuerung basierende Sicherheit. Hierbei werden eingeschränkt: Aufträge basierend auf Farbverwendungsrichtlinie, Dokumententyp, Auftragskosten, Tageszeit, Zugriffskontrolle für Benutzergruppen, Duplexrichtlinie, erlaubten Jobimpressionen und Druckquoten.

Hinweis: Die Verwendung von SNMP durch eine beliebige Xerox® Remote Services-Anwendung stellt kein Sicherheitsrisiko für die IT-Umgebung eines Clients dar, da der gesamte SNMP-basierte Datenverkehr, der von diesen Anwendungen generiert oder verbraucht wird, im Intranet des Clients hinter der Firewall auftritt. Der Windows SNMP-Dienst und der Windows SNMP Trap-Dienst sind im Windows-Betriebssystem standardmäßig nicht aktiviert.

Corporation Security Mode

Die ***geplante*** Synchronisierung der Xerox Device Agent Application mit dem sicheren Kommunikationsserver ist standardmäßig auf *täglich* eingestellt. Beachten Sie, dass die Tageszeit auf eine gewählte Zeit eingestellt werden kann.

Es gibt zwei Corporation Security Modi für Unternehmen: **Normal** und **Locked Down.**

Wenn der Modus**Normal** eingestellt ist, kontaktiert die Device Management Application täglich den Xerox Services Manager.Einstellungen können aus der Ferne geändert werden, ohne dass Vor-Ort-Besuche erforderlich sind, auch wenn die Abfragezeitpläne ausgeschaltet sind. ***(Empfohlener Modus***).

Im Locked-Down-Modus gibt es neben der druckerbezogenen Datensynchronisation keine Kommunikation mit den Kommunikationsservern und die Einstellungen müssen vor Ort geändert werden. Darüber hinaus werden die IP-Adressen des Xerox-Geräteagenten und des Druckers nicht an den Kommunikationsserver gemeldet. Dieser Modus beschränkt alle anderen Vorteile der Fernwartung auf automatisierte Abrechnung und Lieferungen sowie Diagnosedaten, die für den technischen Support verwendet werden.

Hinweis: Wenn eine Xerox Device Agent-Version die Registerkarte Corporation Security Mode nicht enthält, arbeitet sie im Normalmodus.

10. Network Impact

Richtlinien des Unternehmensnetzwerkes aktivieren oder deaktivieren in der Regel bestimmte Netzwerkports auf Routern und/oder Servern. Die meisten IT-Abteilungen haben Bedenken, wenn Ports durch die Anwendung für den ausgehenden Datenverkehr verwendet werden. Die Deaktivierung bestimmter Ports kann die Funktionalität der Anwendung beeinträchtigen. In der folgenden Tabelle finden Sie spezifische Ports, die von den Prozessen der Anwendung verwendet werden. Wenn die Anwendung über mehrere Netzwerksegmente oder Subnetze hinweg scannen muss, müssen Router die Protokolle zulassen, die diesen Portnummern zugeordnet sind.

Protokolle, Ports & andere verwandte Technologien

Tabelle 7 Liste der Protokolle, Ports und Technologien, die in Xerox® Remote Services verwendet werden:.

Port-Nummer	Protokoll	Nutzungsbeschreibung	Datenfluss im Netzwerk
Abhängig von Protokollen der oberen Ebene	**Internet Protocol (IP)**	**Zugrundeliegender Transport für alle Datenkommunikationen**	**Intern + Extern (nur nach Extern)**
NA	Internet Control Message Protocol (ICMP)	Erkennung von Druckern + Fehlerbehebung	Intern
25	Simple Mail Transport Protocol (SMTP)	Drucker + Remote Proxy-App E-Mail-Benachrichtigungen	Intern
53	Domain Name Services (DNS)	Verwendet für DNS-basierte Drucker-Erkennungsoperationen	Intern
80	Hyper Text Transport Protocol (HTTP)	Abfragen der Drucker-Web-Seite und der Device Management Application	Intern
135	Remote Procedure Call (RPC)	Druckererkennung	Intern
161	Simple Network Management Protocol (SNMP v1 / v2C / v3)	Industriestandardprotokoll zur Erkennung von Netzwerkdruckern + Status, Zähler & Lieferdaten abrufen + Druckerkonfiguration abrufen & anwenden. Standard-Community-Namen = “public” (GET), “private” (SET)	Intern

Port-Nummer	Protokoll	Nutzungsbeschreibung	Datenfluss im Netzwerk
443	Hyper Text Transport Protocol Secure (HTTPS)	Sichere Abfragen der Drucker-Webseiten (falls konfiguriert) und der Remote Proxy-Webseite (falls konfiguriert) + Druckerdatenübertragung zurück zu den Xerox® Communication Servers und Kommunikation der Druckkontrollen zurück zum Xerox® Device Manager	Intern + Extern (nur nach Extern)
515, 9100, 2000, 2105	TCP/IP LPR & Raw Port Druckauftragsüber-mittlung	Aktualisierung der Druckersoftware und Diagnose des Testseitendruckes	Intern

11. Security Best Practices

- Halten Sie Drucker immer auf dem neuesten Stand mit der neuesten Firmware/Software. Xerox überwacht Schwachstellen genau und stellt Kunden bei Bedarf proaktiv Sicherheitspatches und Updates zur Verfügung.
- Deaktivieren Sie ungenutzte Ports und Protokolle auf Druckern, wo immer dies möglich ist. Dies geschieht typischerweise an der Web-Benutzeroberfläche (UI) bei Druckern der Büroklasse und der lokalen Benutzeroberfläche (UI) bei Druckern der Produktionsklasse.
- Verwenden Sie, falls verfügbar, Funktionen zur Benutzerzugriffskontrolle auf Druckern. Dies geschieht typischerweise an der Web-Benutzeroberfläche (UI) bei Druckern der Büroklasse und der lokalen Benutzeroberfläche (UI) bei Druckern der Produktionsklasse.
- Verwenden Sie sichere Protokolle, wenn möglich. Dies geschieht typischerweise an der Web-Benutzeroberfläche (UI) bei Druckern der Büroklasse und der lokalen Benutzeroberfläche (UI) bei Druckern der Produktionsklasse.
- Aktivieren Sie Sicherheitsfunktionen, die in das Gerät integriert sind (z. B. Abbilddatei-Datenüberschreibung, Scan-Datenverschlüsselung, Druckschlangenverschlüsselung, Festplattenverschlüsselung, sicherer Druck, verschlüsselte .pdf, CAC/PIV-Zugriffsauthentifizierung).

Weitere Informationen zur Fernwartung@ Xerox finden Sie unter Xerox.com/RemoteServices.

Weitere und spezifische Informationen zu den Sicherheitsmechanismen und -funktionen der Angebotspalette der Xerox Device Management-Applications finden Sie in den jeweiligen Anleitungen:

Xerox Device Agent

Xerox Device Manager

Centre Ware Web

Ob Geräte- oder Content-Sicherheit - Xerox steht mit proaktiver Sicherheit für die neuen Bedrohungen von heute an der Spitze. Besuchen Sie www.xerox.com/security, um auf eine ganze Reihe von Sicherheitsinformationen, updates, bulletins, white papers, patches and more zuzugreifen.