Xerox® Remote Services

Whitepaper zur Datensicherheit

Version 2.0

Globale Remote Services

Xerox® Technology Information Management

Januar 2017

BR19369

An diesem Dokument werden regelmäßig Änderungen vorgenommen. Änderungen, technische Ungenauigkeiten sowie orthografische und typografische Korrekturen werden in den jeweils nachfolgenden Versionen berücksichtigt.

IS 614672/IS 514590

Dokumentversion: 2.0 (Januar 2017).

Inhaltsverzeichnis

Allgemeiner Zweck und Zielgruppe

Dieses Dokument dient als Leitfaden beim Einsatz von Xerox® Remote Services für vernetzte Xerox- und Nicht-Xerox-Drucker in der Kundenumgebung. Es soll Einzelheiten zur Sicherheit und ein Verständnis für die umfangreichen Sicherheitsmaßnahmen liefern, die in den Xerox® Remote Services implementiert werden.

Die Zielgruppen für dieses Dokument sind Technologieanbieter, IT-Netzwerkmanager und IT-Sicherheitsteams, die an den Remote Services-Fähigkeiten und der Sicherheitsimplementierung dieser Funktionen interessiert sind.

Es wird empfohlen, das Dokument vollständig durchzulesen, bevor Xerox® Produkte und Dienstleistungen zur Nutzung in einer vernetzten Kundenumgebung zertifiziert werden.

Remote Services

Informationen sind ein wesentliches Gut und ihr Schutz ist für alle unternehmerischen Vermögenswerte, einschließlich vernetzte Multifunktionsdrucker (MFD), von zentraler Bedeutung. In den „All-in-One"-Konstrukten von heute stellt das Verwalten einer Flotte von Multifunktionsdruckern, bei gleichzeitiger Sicherung einer akzeptablen Sicherheitsstufe, ganz eigene Herausforderungen dar, die häufig übersehen werden. Xerox® liegt das Sicherheitsbedürfnis der Kunden in seiner ganzen Komplexität am Herzen. Xerox® Produkte, Xerox® Systeme und Xerox® Remote Services sind darauf ausgelegt, sich nahtlos in die vorhandenen Arbeitsabläufe Ihres Unternehmens zu integrieren und setzen gleichzeitig aktuellste Sicherheitstechnologien ein.

Das Whitepaper zur Datensicherheit der Xerox® Remote Services hilft den Kunden die entsprechende Sicherheitslösung für Remote Services zu verstehen und einzusetzen, die mit ihrer Netzwerkinfrastruktur kompatibel ist. Es hängt vom Aufbau des Kundennetzwerks ab, ob Änderungen an der Internet-Firewall, an Web-Proxy-Servern oder einer anderen sicherheitsbezogenen Netzwerkinfrastruktur notwendig sind. Welche Lösungen, Geräte und Steuerungen der Xerox® Remote Services ausgewählt werden, hängt von den Kundenrichtlinien zur Informationssicherheit ab und diese Richtlinien bestimmen auch die verwendete Betriebsart.

Die Xerox® Remote Services sind in bestimmten Anlagenmodellen verfügbar. Mit dieser Fähigkeit können Druckgeräte über folgende Druckerattributdaten entfernt gewartet und unterstützt werden*: Identität, Eigenschaften und Status des Druckgeräts, Status der Verbrauchsmaterialien, Verbrauchsdaten und detaillierte Diagnosedaten*. Die Druckerattributdaten werden in Ihrer Netzwerkumgebung direkt vom Druckgerät (Device Direct), durch eine gehostete Anwendung (Device Management-Anwendung) oder über eine Kombination der beiden Methoden mithilfe des sicheren Xerox® Remote Services-Kommunikationspfades übermittelt. Sowohl die Xerox® Geräte als auch das Xerox® Geräteverwaltungssystem haben ein Zertifikat, das mit den Xerox®Communication Servern authentifiziert, bevor eine Übertragung der Druckeigenschaften erfolgen kann. Xerox® Remote Services-Transaktionen gehen stets von der Kundenumgebung aus und zwar basierend auf Autorisierungen durch den Kunden.

Die Xerox® Communication Server in den Vereinigten Staaten stimmen mit den strengen Sicherheitsanforderungen für Informationssicherheitsverwaltung überein. Xerox® Datencenter und Xerox® Remote Services-Anwendungen halten die jährliche Erklärung zu den Konformitätsanforderungen (SSAE - Statement on Standards for Attestation) No-16 und Sarbanes-Oxley Act (SOX) ein und sind ISO 27001:2013 zertifiziert.

Standardmäßig werden weder Druck-, Fax-, Scan-, Kopierabbildungen noch persönliche Informationen des Kunden an die Xerox® Communication Server übermittelt.

Kundensteuerungen

Xerox® Device Management-Anwendungen haben zu Audit- und Verifizierungszwecken die Fähigkeit Datenprotokolle der exportierten Druckerattribute vor der Verschlüsselung und Übertragung an die Xerox® Communication Server anzuzeigen. Siehe das Benutzerhandbuch der jeweiligen Xerox® Device Management-Anwendung für Einzelheiten.

Einige kleine und mittlere Bürodruckgeräte sind mit einer Funktion ausgestattet, mit der die Kunden über die Device Direkt-Methode die Druckerattributdaten vor Verschlüsselung und Übertragung an die Xerox® Communication Server herunterladen und anzeigen können. Um zu überprüfen, ob ein bestimmtes Druckgerät diese Fähigkeit besitzt, muss die Centreware Internet Services-Seite des Druckgeräts aufgerufen werden; danach Status-Register, die Verknüpfung Smart eSolutions (oder Remote Services) und das Register „Wartungsassistent feststellen".

Die Xerox® Remote Services-Lösung kann auf die Kundenrichtlinien zur Informationssicherheit zugeschnitten werden, die bestimmte Arten von Druckerattributen, die außerhalb des Netzwerks übertragen werden können (z. B. Attribute der Netzwerkadresse), streng begrenzen oder beschränken. Mit den Xerox® Device Management-Anwendungstools können ausgewählte Felder vor der Übertragung deaktiviert werden.

Die Kunden haben außerdem die Option, während der Vertragsverhandlungen einen *Ausnahmeantrag* aufzurufen, um sich von der Remote Services-Lösung abzumelden (**„opt-out"**). Mit dieser Option wird die Remote Services-Kommunikation und Remote-Unterstützungsfähigkeit für die Druckgeräte in diesem Konto verhindert.

Um eskalierte Remote-Unterstützungsmaßnahmen zu erleichtern, können Sie bei Bedarf die Remotezugriff-Funktion aktivieren, um Softwareversionen, Sicherheits-Patches und Ferndiagnose für das Druckgerät zu erhalten, Druckgerätkonfigurationen zu reparieren oder modifizieren, damit Diagnosefehler korrigiert werden können. Über den Remotezugriff kann Xerox® keine Kundendokumente, Daten oder andere Informationen, die sich im Druckgerät befinden oder das Gerät durchlaufen, oder Kundeninformationssysteme anzeigen oder herunterladen. Eine Ausnahme besteht, wenn ein Kunde gemeinsam mit dem Xerox-Kundendienst an einem schwierigeren Problem arbeitet und wenn dabei festgestellt wird, dass für die Beseitigung des Problems weitere Informationen erforderlich sind. Zu diesem Zeitpunkt kann sich der Kunde entschließen, Xerox den Zugriff auf örtlich im Gerät gespeicherte Protokolle, die sensible Daten enthalten, zu erlauben.

Deshalb werden IT-Teams des Unternehmens und Sicherheitsfachleute aufgefordert dieses Dokument vollständig zu lesen, damit sie wirklich die verschiedenen Funktionen, Anforderungen und Operationen der Xerox® Remote Services verstehen und wie die Remote Services die Einhaltung der Kundenrichtlinien zur Informationssicherheit unterstützen.

Zusätzliche Sicherheitsressourcen für Xerox® Produktsicherheitsdatenschutz, Industriepartnerschaften und Zertifizierungen sind unter http://www.xerox.com/security zu finden.

Einsatzmodelle

Sie können zwischen folgenden gleichermaßen sicheren Einsatzmodellen der Xerox ® Remote Services wählen:

- **Modell „Device Direct“** - Mit Device Direct können Druckgeräte durch die Kunden-Firewall über das Internet direkt mit den entfernten Xerox® Communication Servern kommunizieren.

- **Modell „Device Management-Anwendung“** - Mit einer Xerox® Device Management-Anwendung (auch Device Manager) kann im Kundennetzwerk aus den Druckgeräten eine Teilmenge von Datenattributen gesammelt werden. Mehrere Druckerattribute werden gesammelt und dann sicher an die entfernten Xerox® Communication Server übermittelt.

- **Kombiniertes Modell** – Die Implementierung beider Modelle „Device Direct“ und „Device Management-Anwendung“.

Alle Einsatzmodelle für Xerox ® Remote Services nutzen für einen sicheren, verschlüsselten Kanal webbasierte Industriestandard-Protokolle und -Ports, um die Attribute der Druckgeräte extern an die Xerox® Communication Server zu übertragen, die sich in redundanten Xerox® Datencentern befinden.

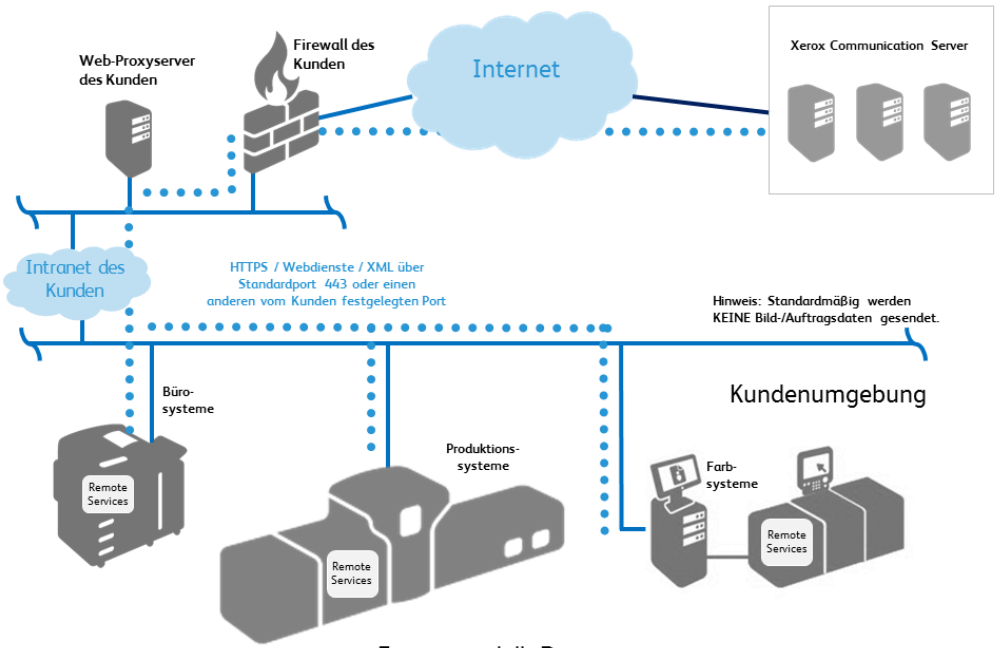
Welches Einsatzmodell gewählt wird, hängt von den Kundenrichtlinien und Regeln zur Informationssicherheit für das Handhaben der Übertragung der Druckerattribute ab und von der Art der Druckdienstlösung und den Geräten, die von Xerox® gekauft werden (Basis oder Managed Print Services).

Einsatzmodell „Device Direct“

Das in Xerox®-Geräte eingebettete Remote Services-Modul nutzt einen sicheren TLS 1.2-Anschluss über den Standardport 443, um extern mit den entfernten Xerox® Communication Servern zu kommunizieren.

- Druckgeräte in der Kundenumgebung initiieren alle Kommunikationen direkt mit den entfernten Xerox® Communication Servern. Um die Kommunikation zu aktivieren, sind Standardkonfigurationen für die Firewall erforderlich.
- Es muss eine gültige URL für die entfernten Xerox® Communication Server verwendet werden.
- Die Xerox® Communication Server befinden sich hinter einer sicheren Firewall und sind nicht über das Internet zugänglich.

Abb.1



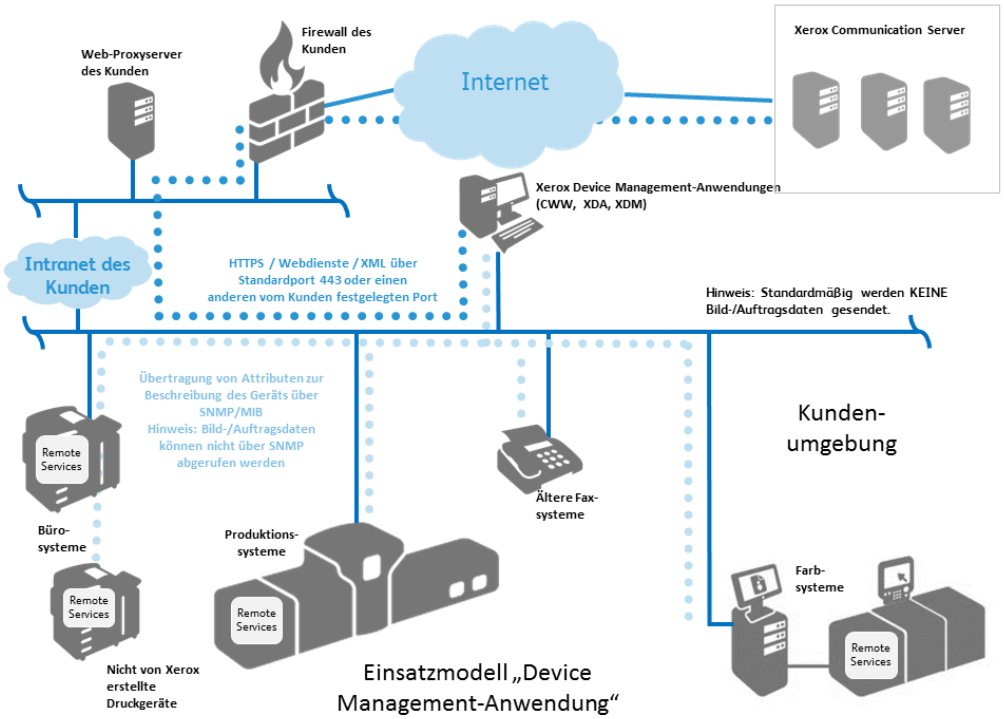
Einsatzmodell „Device Direct“

Einsatzmodell „Device Management-Anwendung“

Die Device Management-Anwendung (d. h. **Xerox® Centre Ware® Web, Xerox® Device Agent, Xerox® Device Agent Partner Edition und Xerox® Device Manager)** nutzen auch einen sicheren, verschlüsselten TLS 1.2-Anschluss über den Standardport 443, um extern mit den entfernten Xerox® Communication Servern zu kommunizieren. Um die Sicherheit über diesen Kanal zu verbessern, werden zusätzliche Funktionen genutzt und während der Anfangsinstallation der Device Management-Anwendung aufgebaut. Diese Funktionen sind:

- Die Device Management-Anwendung in der Kundenumgebung initiiert alle Kommunikationen direkt mit den entfernten Xerox® Communication Servern. Um die Kommunikation zu aktivieren, sind Standardkonfigurationen für die Firewall erforderlich.
- Es muss eine gültige URL für die entfernten Xerox® Communication Server verwendet werden.
- Die Xerox® Communication Server befinden sich hinter einer sicheren Firewall und sind nicht über das Internet zugänglich.
- Es müssen entweder eine gültige Konto-ID oder eine Site-Kennung und ein Xerox® Communication Server-Registrierungsschlüssel verwendet werden, um auf einige der Dienste auf den Xerox® Communication Servern zuzugreifen.
- Für die Device Management-Anwendung muss mithilfe des geeigneten Berechtigungsnachweises für die Zertifikatsauthentifizierung eine Registrierung mit den Xerox®Communication Servern erfolgen.
- Die angegebenen Berechtigungen werden von den entfernten Xerox® Communication Servern geprüft und die Anträge akzeptiert.
- Die Device Management-Anwendung authentifiziert die entfernten Xerox® Communication Server und aktiviert den Dienst.

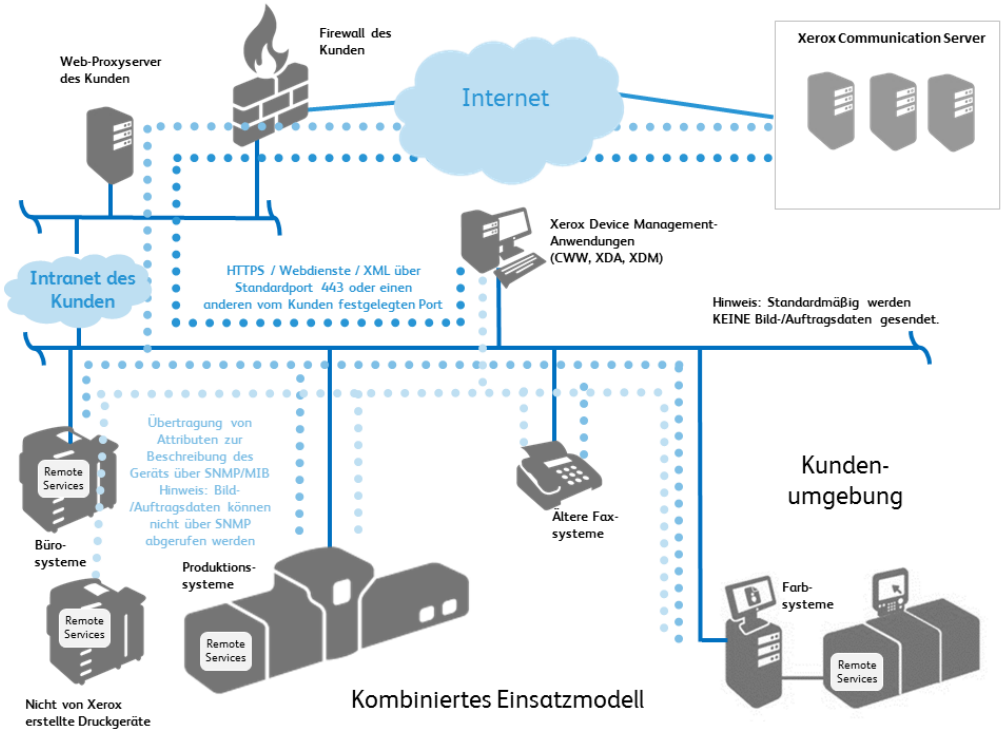
Abb.2



Kombiniertes Einsatzmodell

Der kombinierte Einsatz wird verwendet, wenn ein Kunde für seine Druckgeräte mehrere Arten von Xerox-Wartungsverträgen erworben hat. Wenn ein Xerox® Druckgerät anfänglich in einem Netzwerk installiert wird, dann versucht das Druckgerät gemäß des standardmäßigen Verhaltens der Xerox® Remote Services, eine direkte Verbindung mit den Xerox® Communication Servern aufzubauen.

Figure 3



Datenübertragung und Nutzlasten

Datenquellen

Die Druckerdatenattribute werden von folgenden Quellen für Xerox® Remote Services gesammelt:

- Xerox® Büronetzwerkdrucker
- Nicht-Xerox® Netzwerkdrucker
- Xerox® Produktionsdrucker
- Xerox® Device Management-Anwendungen

Xerox® Bürogeräte

Xerox® Druckgeräte der Büroklasse übertragen die Gerätedatenattribute in XML (eXtensible Markup Language)-Format mittels einer komprimierten .zip-Datei. Jede Datei wird dann über einen verschlüsselten Kanal an die entfernten Xerox® Communication Server übermittelt.

Tabelle 1 identifiziert das Gerätedatenattribut, das übermittelt werden kann, und dessen Beschreibung.

Datenattribute	Beschreibung
Druckgeräteidentität	Umfasst Modell, Firmware-Level, Seriennummern der Module und das Installationsdatum.
Netzwerkadresse des Druckgeräts	Umfasst MAC-Adresse, Subnetz-Adresse.
Druckgeräteeigenschaften	Umfasst die detaillierte Hardware-Konfiguration, die detaillierte Konfiguration der Softwaremodule, unterstützte Funktionen und Dienste, Energiesparmodi usw.
Druckgerätestatus	Umfasst den allgemeinen Status, detaillierte Alarme, die letzten 40 Fehlereinträge, Papierstaudaten usw.
Druckgerätezähler	Umfasst Rechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, faxbezogene Zähler, Zähler für große Aufträge, Zähler für Scan-auf-Ziel-Aufträge, Nutzungsstatistiken usw.
Verbrauchsmaterialien der Druckgeräte	Umfasst den Namen und die Art von Verbrauchsmaterialien (z.B. Bildverarbeitung, Endbearbeitung, Papiermedien), Füllstand, Kapazität, Status, Größe usw.

Datenattribute	Beschreibung
Druckeinzelheiten der Gerätenutzung	Umfasst detaillierte druckbezogene Zähler, Einschaltstatus, detaillierte CRU-Austauschmengen, detaillierte CRU-Fehlerdaten und -verteilungen, Verwendung der eingebetteten OCR-Funktionen, Druckauflagenverteilung, Nutzungsverteilung der Papierbehälter, installierte Medien, Verteilung der Medienarten, Verteilung der Mediengrößen, Verteilung der Dokumentenlängen, Verteilung von Satznummern, SFWB-Daten und NVM-Daten, Anzahl markierter Pixel, durchschnittliche Flächenabdeckung pro Farbe, Fehler/Papierstaus, detaillierte scanbezogene Zähler.
Engineering / Debug (Technik/Fehlerbeseitigung)	Umfasst detaillierte Debug-Informationen, die Daten außerhalb des oben gelisteten Datensatzes enthalten können. Diese Daten können PII (personenbezogene Daten), z. B. Benutzernamen, E-Mail-Adressen und Auftragsdaten enthalten. Diese Daten werden mit ausdrücklichem Einverständnis des Kunden gesendet und sind nur für eskalierte Unterstützungsmaßnahmen gedacht.

Hinweis: Die Datei und der Inhalt der identifizierten Daten hängen vom Produktmodell ab.

Xerox® Produktionsgeräte

Xerox® Geräte der Produktionsklasse übertragen die Gerätedatenattribute in XML (eXtensible Markup Language)-Format mittels einer komprimierten .zip-Datei. Jede Datei wird dann über einen verschlüsselten Kanal an die entfernten Xerox® Communication Server übermittelt.

Tabelle 2 identifiziert die Gerätedatenattribute und deren Beschreibung, die übermittelt werden können.

Datenattribute	Detaillierte Beschreibung der Datenattribute
Druckgeräteidentität	Umfasst Modell, Firmware-Level der Module, Seriennummern der Module, Installationsdaten der Module, Kundenkontaktdaten, Lizenzdaten und Standort, falls vorhanden.
Netzwerkadresse des Druckgeräts	Umfasst MAC-Adresse, Subnetz-Adresse.
Druckgeräteeigenschaften	Umfasst die detaillierte Hardware-Konfiguration, die detaillierte Konfiguration der Softwaremodule, unterstützte Funktionen und Dienste usw.
Druckgerätestatus	Umfasst aktive Stati, Anzahl von Fehlereinträgen, DFE-Ereignisprotokoll, Datenübertragungsverlauf
Druckgerätezähler	Umfasst Rechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, auftragsbezogene Zähler, produktionsspezifische Zähler, Zähler für Scan-auf-Ziel-Aufträge auf Produktionsmodellen des unteren Marktsegments usw.
Verbrauchsmaterialien der Druckgeräte	Umfasst Hersteller, Modell, Seriennummer, Name, Art, Füllstand, Kapazität, Status, Standzeitzähler
Druckeinzelheiten der Gerätenutzung	Umfasst HDSI-Daten, NVM-Daten, Teileaustausch, DFE-Protokolle, detaillierte Diagnosedaten, Fehlerbehebung.
Engineering / Debug (Technik/Fehlerbeseitigung)	Umfasst nicht strukturierte, detaillierte Daten zur Fehlerbehebung, nur für Level 3-Support.
Kundenauftragsbezogen	Mit Xerox® Produktionsdruckprodukten besteht die Fähigkeit auftragsbezogene Daten zur Unterstützung von eskalierten Support-Szenarien über verschlüsseltes PostScript an Xerox zu reproduzieren. Es liegt im Ermessen des Kunden, ob er diese Funktion aktiviert oder nicht. Sollte der Kunde sich entschließen auftragsbezogene Daten (d. h. verschlüsseltes PostScript) an Xerox zu übermitteln, werden diese Daten gemäß den Xerox-Richtlinien und -Standards zur Informationssicherheit behandelt.

Eskalierte Support-Szenarien liegen dann vor, wenn detaillierte Debug-Informationen gegeben sind, die Datenattribute außerhalb des in den Tabellen 1-3 festgelegten Datensatzes umfassen. Diese Daten werden mit ausdrücklichem Einverständnis des Kunden gesendet und werden gemäß den Xerox-Richtlinien und -Standards zur Informationssicherheit behandelt.

Hinweis: Die Datei und der Inhalt der identifizierten Daten hängen vom Produktmodell ab.

Xerox® Device Management-Anwendungen

Die Xerox® Device Management-Anwendungen (d. h. Xerox® Centre Ware® Web (**CWW**), Xerox® Device Agent (**XDA**) , Xerox Device Agent Partner Edition (**XDA PE**) und Xerox® Device Manager (**XDM**) übermitteln die Druckattributdaten in XML (eXtensible Markup Language)-Format mittels einer komprimierten .zip-Datei. Die Datei wird dann verschlüsselt und über verschlüsselte Kanäle an die entfernten Xerox® Communication Server übermittelt.

Tabelle 3 identifiziert die Gerätedatenattribute und deren Beschreibung, die über die Xerox® Device Management-Anwendung übermittelt werden können.

Datenattribute	Detaillierte Beschreibung der Datenattribute
Druckgeräteidentität	Umfasst Hersteller, Modell, Beschreibung, Firmware-Level, Seriennummer, Ressourcenkennzeichen, Systemnamen, Kontakt, Standort, Verwaltungsstatus, Arbeitsstation (Desktop), Fax-Telefonnummer und Warteschlangennamen.
Netzwerkadresse des Druckgeräts	Umfasst MAC-Adresse, IP-Adresse, DNS-Name, Subnetzmaske, IP-Standardgateway, letzte bekannte IP-Adresse, IP-Adresse geändert, Zeitzone, IPX-Adresse, IPX-Externe Netzwerknummer, IPX-Druckserver.
Druckgeräteeigenschaften	Umfasst installierte Komponenten, Komponentenbeschreibungen, unterstützte Funktionen und Funktionen, Druckgeschwindigkeit, Farbsupport, Endbearbeitungsoptionen, Duplex-Support, Markierungs- und Kennzeichnungstechnik, Festplatte, RAM, Sprachensupport, benutzerdefinierte Eigenschaften.
Druckgerätestatus	Umfasst den allgemeinen Status, detaillierte Alarme, lokale Konsolennachrichten, Komponentenstatus, Daten im Zusammenhang mit der Datenabholung. Erkennungsdatum, Erkennungsmethode/-art, Betriebszeit des Geräts, Traps unterstützt/aktiviert.
Druckgerätezähler	Umfasst Rechnungszähler, druckbezogene Zähler, kopierbezogene Zähler, faxbezogene Zähler, Zähler für große Aufträge, scanbezogene Zähler, Nutzungsstatistiken und Zielmenge.
Verbrauchsmaterialien der Druckgeräte	Umfasst den Namen und die Art von Verbrauchsmaterialien (z.B. Bildverarbeitung, Endbearbeitung, Papiermedien), Füllstand, Kapazität, Status, Größe usw.
Detaillierte Nutzung der Druckgeräte	Benutzerbezogene Auftragsverfolgungsdaten, die Auftragscharakteristiken (ID, Dokumentname, Eigentümer, Dokumentenart, Auftragsart, Farbe, Duplex, erforderliche Medien, Größe, Seiten, Sätze, Fehler), Ziel (Druckgerät, Modell, DNS-Name, IP-Adresse, MAC-Adresse, Seriennummer), Ergebnisse des Druckauftrags (Absetzzeit, Druckzeit des Auftrags, gedruckte Seiten, Seiten gedruckt in Farbe/Schwarzweiß, verwendeter Farbmodus, N-up), Buchhaltungsdaten (Rückbuchungscode, Rückbuchungspreis, Buchhaltungsquelle), Quelle des Druckauftrags (Arbeitsstation, Druckservername/MAC-Adresse, Warteschlangenname, Port, Benutzername, Benutzer-ID), Xerox-Verwaltungsdaten (an Xerox® Services Manager gesendet).

Datenattribute	Detaillierte Beschreibung der Datenattribute
Device Manager-Identität	Umfasst PC-Informationen des Anwendungs-Hosts, z.B. DNS-Name, IP-Adresse, BS-Name, BS-Typ, PC CPU, RAM-Größen (frei gegenüber benutzt), Festplattengrößen (frei gegenüber benutzt), Standortname, App-Version, App-Lizenzablaufdatum, .Net-Version, Zeitzone, Erkennung der Komponentenversion, Größe der Hauptdatenbank, Größe der Erkennungsdatenbank, Anzahl der Drucker/im Umfang/nicht im Umfang, laufende kritische Dienste.
Device Manager Sicherheitsmodus für Unternehmen	**Normaler Modus** = Xerox® Device Agent kontaktiert täglich den Xerox® Services Manager. Einstellungen können ohne Besuche vor Ort entfernt geändert werden, selbst wenn Abfragezeitpläne ausgeschaltet sind. **Sperrmodus (Lock Down Mode)** = Außer Drucker-bezogener Datensynchronisation besteht keine Kommunikation mit Xerox® Services Manager und Einstellungen müssen vor Ort geändert werden. Xerox® Device Agent-Gerät und IP-Adresse des Druckers werden an Xerox® Services Manager berichtet.
Device Manager - Richtlinie zur Drucksteuerung	Umfasst PC-Name des Endbenutzers, verwendeter Druckserver, Druckwarteschlange, verwendete Druckwarteschlange, Zeitstempel des Verstoßes, Dokumentenname, Benutzername des Endbenutzers, Duplex-Auftrag, Farbauftrag, Gesamtanzahl der Auftragsausdrucke, Auftragspreis, durchgeführte Aktion, Endbenutzer benachrichtigt, Meldung angezeigt, Name der Druckrichtlinie, Regel der Druckrichtlinie.

Entfernte Verwaltung von Druckgeräten

Xerox® Supportpersonal kann die folgenden Maßnahmen durch die Xerox® Device Management-Anwendung durchführen. Wenn zulässig, werden diese Maßnahmen zur Unterstützung einer Abweichungsauflösung durchgeführt und sind unten in **Tabelle 4** dargestellt.

Daten	Beschreibung
Auf Druckgeräten durchzuführende Aktionen	• **Gerätestatus holen** = Abholen des letzten Status des Druckgeräts • **Gerät neu starten** = Initiieren einer Ausschalt-/Einschaltsequenz für das Druckgerät • **Gerät aktualisieren** = Installieren neuer Software/Firmware auf dem Druckgerät (.DLM über Port 9100) • **Gerätefehler beseitigen** = Gerät pingen + Abholen des letzten Status des Druckgeräts • **Testseite drucken** = Absetzen eines Testauftrags an ein Druckgerät, um den Druckpfad zu überprüfen (einen Konfigurationsbericht erstellen) • **Geräteverwaltung starten** = Initiieren periodischer Übertragungen der Druckgerätedaten an die externen Xerox® Communication Server **Hinweis:** Jede Aktion kann bei Bedarf innerhalb des Teils der Verwaltungskonfiguration der Xerox® Device Management-Anwendungen, die diese Funktion unterstützen, deaktiviert werden.
Auf Druckgeräten durchzuführende Aktionen	• **Gerät neu starten** = Initiieren einer Ausschalt-/Einschaltsequenz für das Druckgerät • **Testseite drucken** = Absetzen eines Testauftrags an ein Druckgerät, um den Druckpfad zu überprüfen (einen Konfigurationsbericht erstellen)
Maßnahmen, die auf den Device Management-Anwendungen durchgeführt werden	Einstellungen innerhalb jeder Device Management-Anwendung, die verwaltet werden können, umfassen den Erkennungsprozess, Frequenz des Datenexports, Einstellungen hinsichtlich der SNMP-Kommunikation (Wiederholung, Zeitüberschreitung, Community-Name), Alarmprofile und die automatische Softwareupdate-Frequenz der Device Management-Anwendung.

Systemanforderungen für Device Management-Anwendungen

Abhängig von den Angeboten unterscheiden sich die Mindestanforderungen etwas. Basisanforderungen speziell für die jeweilige Device Management-Anwendung befinden sich in Benutzerhandbuch, Sicherheitsevaluierungsleitfaden und/oder Zertifizierungsleitfaden. Zusätzliche Einzelheiten sind zu finden unter:
http://www.support.xerox.com/support/enus.html

Bei der Installation wird eine .readme-Datei eingefügt, die zusätzliche und spezifische Systemanforderungen für die jeweilige Device Management-Anwendung, die installiert wird, anspricht.

- Es wird empfohlen, dass Host-Computer ein unterstütztes Betriebssystem von Microsoft ® Corporation ausführen. Die Xerox® Device Management-Anwendungen können aber auch in einem Macintosh Betriebssystem ausgeführt werden, wenn Emulations-Software von Parallels Desktop verwendet wird. (In einer nativen Macintosh-Umgebung kann die Xerox® Device Management-Anwendung aktuell nicht ausgeführt werden.) Siehe die Benutzerhandbücher der jeweiligen Xerox® Device Management-Anwendung für zusätzliche Einzelheiten.

- Es wird empfohlen, Host-Computer mit den aktuellsten kritischen Patches und Serviceversionen von Microsoft ® Corporation auf dem Laufenden zu halten.

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

- Eine Internetverbindung ist notwendig

- Zum Installieren der Device Management-Anwendung auf dem Client-Gerät werden Administratorrechte benötigt.

- Erfordert SNMP-aktivierte Geräte und die Fähigkeit SNMP über das Netzwerk zu senden. Es ist nicht notwendig SNMP in dem Computer, in dem Xerox® Device Management-Anwendungen installiert werden, oder in anderen Netzwerkcomputern zu aktivieren.

- Microsoft®.NET Framework 4.6 (Vollversion) muss vor der Anwendung installiert werden.

- Die Anwendung sollte nicht auf einem Computer installiert werden, auf dem andere SNMP-Anwendungen oder andere Xerox® Device Management-Tools installiert sind, da diese den Betrieb des jeweils anderen Programms stören können.

Nicht unterstützte Konfigurationen

- Installation der Anwendung in einem Computer mit einer anderen Xerox® Device Management-Anwendung, wie Xerox® Device Manager.

- Unix® oder Linux® Betriebssystem

- Microsoft ® Betriebssysteme, die am Ende ihrer Lebensdauer stehen, z. B. Windows NT® 4.0, Windows® Media Center, Windows® XP und Windows® Server 2000 und 2003.

- Virtuelle Umgebungen anders als VMware® Lab Manager™/Workstation/vSphere Hypervisor™. Diese Anwendung funktioniert möglicherweise in anderen virtuellen Umgebungen; diese Umgebungen wurden jedoch nicht getestet.

Xerox® Geschäftsprozesse und Dienste

Die in den Xerox® Communication Servern von Xerox® Bürodruckgeräten, Xerox® Produktionsdruckgeräten und Xerox® Device Management-Anwendungen empfangenen Daten werden von den folgenden Xerox Geschäftsprozessen genutzt:

Name des Geschäftsprozesses	Beschreibung
Automatisches Zählerablesen	Aufgrund der von den Druckgeräten erhaltenen Zählerdaten wird automatisch eine Rechnung erstellt.
Automatisches Auffüllen von Verbrauchsmaterialien / Automatisches Auffüllen von Teilen	Der Toner wird den Kunden automatisch zugesandt, wenn der von den Druckgeräten empfangene Status der Verbrauchsmaterialien Erschöpfung anzeigt. Austauschbare Komponenten werden den Kunden automatisch zugesandt, wenn diese für deren Druckgeräte benötigt werden. Diese Optionen stehen nur Kunden zur Verfügung, die sich für Zählerversorgungsverträge entscheiden.
Gebrauchsfähigkeit (Wartungsassistent)	Der Xerox-Kundendienst kann detaillierte Fehlerinformationen bei Bedarf einsehen, um die Vorbereitung auf einen Besuch vor Ort zu beschleunigen oder Probleme entfernt zu diagnostizieren oder zu lösen.
Support Level 3 (Engineering/Debug (Technik/Fehlerbeseitigung))	Produkt-Supportpersonal kann schwierige Probleme untersuchen, wenn ihnen die detaillierten Engineering-/Debugprotokolle zur Verfügung gestellt werden.

Grundlegende Druckgerätedaten werden in einem ISO-27001-zertifizierten Xerox® Datencenter komprimiert, übermittelt, aufbewahrt und archiviert und in Übereinstimmung mit den Aufbewahrungsrichtlinien für Xerox® Unternehmensdaten gehalten.

Die Arbeitsprozesse und Praktiken zur Unterstützung und zum Schutz der Softwaresysteme für Xerox® Back-Office Remote Services basieren auf den bewährten Verfahren der ITIL und den Xerox-Richtlinien zur Informationssicherheit, die wiederum auf den ISO 27001-Normen basieren. Die Kunden können sich sicher sein, dass die Verwaltung von Datenintegrität, Privatsphäre und Schutz mit den bewährten Verfahren übereinstimmen.

Details zur Technologie

Dieser Abschnitt enthält zusätzliche von IT-Teams und Sicherheitsfachleuten üblicherweise benötigte technische Details, die durch die Zusicherung sicherer Entwicklungspraktiken Risiken verwalten sollen und so die Zertifizierung von Druckgeräten und Device Management-Anwendungen für den Einsatz in Kundennetzwerken ermöglichen.

Softwaredesign

Unsere Verantwortung für die Xerox® Produktsicherheit beginnt frühzeitig in der Produktentwicklung mit bewährten Industriestandardverfahren für sicheres Kodieren, umfangreiche Tests und Analysen, um Schwachstellen zu beseitigen. Xerox® bindet Zertifizierungsverfahren, z. B. gemeinsame Kriterien, aktiv ein und engagiert sich für aufkommende Standards, wie die P2600 Arbeitsgruppe und den SDLC (Security Development Lifecycle - Sicherheitsentwicklungszyklus).

Bedienbarkeit

Xerox® Remote Services führt die folgenden Arten von Prozessen in einem Netzwerk aus:

Einsatzmethode	Verwendete Anwendung	Datenfluss im Netzwerk	Einem Netzwerk auferlegte Bedienbarkeit
Geräteidentität	Keine	Intern	Das Xerox® Druckgerät versucht, einen Web-Proxy-Server zu erkennen (automatisch oder an eine bestimmte Adresse verwiesen)
		Intern	Xerox® Druckgeräte können so programmiert werden, dass sie Aufträge an einen SMTP-Server generieren, um E-Mail-Nachrichten mit Alarmmeldungen an eine bestimmte Empfängerliste zu senden.
		Extern zum Netzwerk	Das Xerox® Druckgerät durchquert die Firewall des Unternehmens, um auf das Internet (HTTPS über Port 443) zuzugreifen.
		Extern zum Netzwerk	Das Xerox® Druckgerät authentifiziert sich mit seinem Zertifikat im entfernten Xerox Communication Server, bevor es Datenattribute übermittelt
		Extern zum Netzwerk	Das Xerox® Druckgerät übermittelt täglich zu einer bestimmten Uhrzeit oder nach Aufforderung des Kunden über einen verschlüsselten Kanal (HTTPS über Port 443) Druckerattributdaten automatisch an die Xerox® Communication Server.

Einsatzmethode	Verwendete Anwendung	Datenfluss im Netzwerk	Einem Netzwerk auferlegte Bedienbarkeit
		Extern zum Netzwerk	Das Xerox® Druckgerät fragt bei den Xerox® Communication Servern täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch nach einer Liste von durchzuführenden Aktionen (z.B. Rechnungsdaten jetzt senden, Dienst hinzufügen usw.)
		Extern zum Netzwerk	Einseitige Übertragung der Engineering-Protokolldaten des Xerox® Druckgeräts über einen verschlüsselten Kanal (HTTPS über Port 443) an die Xerox® Communication Server
Device Management-Anwendungen	Centre Ware® Web	Intern	Jede App erkennt einen Web-Proxy-Server (automatisch oder an eine bestimmte Adresse verwiesen)
		Intern	Jede App holt die Funktionen der Druckgeräte der Flotte über SNMP ab
		Intern	Jede App holt die Konfigurationen der Druckgeräte der Flotte über SNMP ab
		Intern	Jede App holt den Status der Druckgeräte der Flotte über SNMP ab
		Intern	Jede App holt die Daten der Verbrauchsmaterialien der Druckgeräte der Flotte über SNMP ab
		Intern	Jede App kann ein Druckgerät über SNMP oder die Web-Benutzeroberfläche des Druckgeräts neu starten
		Intern	Jede App kann eine Testseite an ein bestimmtes Druckgerät absetzen
		Intern	Jede App kann die Webseite eines Druckgeräts aufrufen
		Extern **(nur ausgehend)**	Jede App durchquert den Firewall des Unternehmens, um auf das Internet (HTTPS über Port 443) zuzugreifen
		Extern **(nur ausgehend)**	Jede App authentifiziert sich mit ihrem Zertifikat im entfernten Xerox Communication Server, bevor sie Datenattribute übermittelt
		Extern **(nur ausgehend)**	Jede App überträgt die Attribute des Druckgeräts täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch an die Xerox® Communication Server
		Extern **(nur ausgehend)**	Jede App fragt bei den Xerox® Communication Servern täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch nach einer Liste von durchzuführenden Aktionen
		Intern	Jede Xerox® Device Agent-App erkennt einen Web-Proxy-Server (automatisch oder an eine bestimmte Adresse verwiesen)

Einsatzmethode	Verwendete Anwendung	Datenfluss im Netzwerk	Einem Netzwerk auferlegte Bedienbarkeit
Device Management-Anwendungen	Xerox® Device Agent Partner Edition zum Überwachen von vernetzten Druckgeräten	Intern	Jede Xerox® Device Agent-App holt die Funktionen der Druckgeräte der Flotte über SNMP ab
		Intern	Jede Xerox® Device Agent-App holt die Konfiguration der Druckgeräte der Flotte über SNMP ab
		Intern	Jede Xerox® Device Agent-App holt den Status der Druckgeräte der Flotte über SNMP ab
		Intern	Jede Xerox® Device Agent-App holt die Daten der Verbrauchsmaterialien der Druckgeräte der Flotte 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 Druckgeräts aufrufen
		Intern	Jede Xerox® Device Agent-App kann die Software von Druckgeräten via Absetzung eines Druckauftrags aktualisieren. (.DLM-Datei über Port 9100)
		Extern **(nur ausgehend)**	Jede Xerox® Device Agent-App durchquert die Firewall des Unternehmens, um auf das Internet (HTTPS über Port 443) zuzugreifen
		Extern **(nur ausgehend)**	Jede App authentifiziert sich mit ihrem Zertifikat im entfernten Xerox Communication Server, bevor sie Datenattribute übermittelt
		Extern **(nur ausgehend)**	Jede Xerox® Device Agent-App überträgt die Attribute des Druckgeräts täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch an die Xerox® Communication Server
		Extern **(nur ausgehend)**	Jede Xerox® Device Agent-App fragt bei den Xerox® Communication Servern täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch nach einer Liste von durchzuführenden Aktionen
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps erkennen einen Web-Proxy-Server (automatisch oder an eine bestimmte Adresse verwiesen)
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps holen die Funktionen der Druckgeräte der Flotte über SNMP ab
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps holen die Konfiguration der Druckgeräte der Flotte über SNMP ab
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps holen den Status der Druckgeräte der Flotte über SNMP ab

Einsatzmethode	Verwendete Anwendung	Datenfluss im Netzwerk	Einem Netzwerk auferlegte Bedienbarkeit
Device Management-Anwendungen	Xerox® Device Manager zum Überwachen von vernetzten Druckgeräten	Intern	Xerox® Device Manager / Xerox® Device Agent-Apps holen die Daten der Verbrauchsmaterialien der Druckgeräte der Flotte über SNMP ab
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps können anfordern, dass das Gerät einen Konfigurationsbericht druckt
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps können die Webseite eines Druckgeräts aufrufen
		Intern	Xerox® Device Manager / Xerox® Device Agent-Apps können die Software von Druckgeräten via Absetzung eines Druckauftrags aktualisieren
		Intern	Die Xerox® Device Manager-App unterstützt SNMPv3-Kommunikationen mit Druckgeräten
		Intern	Die Xerox® Device Manager-App kann die Konfiguration des Druckgeräts über SNMP und Web-Benutzeroberfläche ändern
		Intern	Die Xerox® Device Manager-App holt auftragsspezifische Buchhaltungsprotokolle von bestimmten Xerox® MFD ab
		Intern	Die Xerox® Device Manager-App verwaltet / setzt Richtlinien zur Drucksteuerung durch
		Extern **(nur ausgehend)**	Xerox® Device Manager / Xerox® Device Agent-Apps durchqueren die Firewall des Unternehmens, um auf das Internet (HTTPS über Port 443) zuzugreifen
		Extern **(nur ausgehend)**	Jede App authentifiziert sich mit ihrem Zertifikat im entfernten Xerox Communication Server, bevor sie Datenattribute übermittelt
		Extern **(nur ausgehend)**	Xerox® Device Manager / Xerox® Device Agent-Apps übermitteln täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch Druckgerätedaten an die Xerox® Communication Server
		Extern **(nur ausgehend)**	Xerox® Device Manager / Xerox® Device Agent-Apps fragen täglich zu einer bestimmten Uhrzeit über einen verschlüsselten Kanal (HTTPS über Port 443) automatisch Druckgerätedaten bei den Xerox® Communication Servern ab

SNMP (Simple Network Management Protocol)

Das SNMP ist das am meisten verwendete Netzwerkmanagementtool für Kommunikation zwischen Netzwerkverwaltungssystemen und Netzwerkdruckern. Die Device Management-Anwendungen verwenden SNMP während Erkennungsprozessen, um detaillierte Druckgeräteinformationen, die im Netzwerk gefunden wurden, abzurufen. Xerox® Device Management-Anwendungen unterstützen SNMP v1/v2- und v3-Protokolle. Bestimmte Details sind in den jeweiligen Zertifizierungsleitfäden für die Xerox® Device Management-Anwendung zu erfahren.

Das SNMP v3-Framework unterstützt mehrere Sicherheitsmodelle, die in einer SNMP-Einrichtung gleichzeitig vorhanden sein können. Für die strengere Sicherheit in SNMPv3 wurde zu SNMPv2 kryptografische Sicherheit hinzugefügt. Außerdem ist SNMPv3 mit früheren Versionen rückwärts kompatibel und wird häufig über tragfähige Netzwerke verwendet.

Xerox® Device Management-Anwendungen (Centre Ware® Web / Xerox® Device Manager) haben die Fähigkeit mit Geräteplattformen zu kommunizieren, die in ihrer Implementierung von SNMPv3 FIPS 140-2 konform sind.

Die Xerox® Device Management-Anwendungen verwenden weder den Windows SNMP-Dienst noch den Windows SNMP Trap-Dienst. Wenn diese Dienste zuvor installiert wurden, müssen sie auf allen Computern oder Servern, auf denen die Xerox® Device Management-Anwendung installiert ist, deaktiviert werden.

Die Xerox® Device Management-Anwendung nutzt einen von Xerox entwickelten SNMP-Agenten, der:

- Einen speziellen Verschlüsselungs-/Entschlüsselungsmechanismus enthält
- Vollständig via .NET verwaltet wird
- Die zur Laufzeit ausführbare .NET-Datei verwendet, die erweiterte Sicherheit bietet, um Angriffe gegen Softwareschwachstellen, wie ungültige Zeigemanipulationen, Überläufe von Puffern und Indexprüfungen zu verhindern.

Die Xerox® Device Management-Anwendungen nutzen die Sicherheitsfunktionen vom Windows-Betriebssystem einschließlich:

- Authentifizierung und Autorisierung von Benutzern
- Konfiguration und Verwaltung von Diensten
- Einsatz und Verwaltung von Gruppenrichtlinien

Windows Internet Connection Firewall (ICF) einschließlich:

- Sicherheitsprotokolleinstellungen
- ICMP-Einstellungen

Xerox® Device Management-Anwendungen: **Xerox® Device Agent, Xerox® Device Agent Partner Edition oder Xerox® Device Manager** verwenden SQL CE-Anwendung Microsoft® SQL Server

Die Xerox® Device Management-Anwendung kann so konfiguriert werden, dass sie die zusätzlichen Sicherheitsfunktionen der Microsoft® SQL Server-Anwendung verwendet einschließlich:

- Aktivieren der Benutzerkonto-Registrierung
- Verschlüsselung von DNS (Domain Name System)
- Begrenzen von reduzierten Benutzerkontoberechtigungen, um auf die Datenbank zuzugreifen (d.h. Eigentümerberechtigungen für die Datenbank)
- Implementierung von benutzerdefinierten Portnummern

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

Die externen Kommunikationen der Xerox® Device Management-Anwendungen können unter Umständen durch die Windows-Internetverbindungsfirewall beeinträchtigt werden. (Wir **empfehlen**, dass Kunden die Xerox URL in die Whitelist der Kunden-Firewall aufnehmen und die IP-Adresse bestimmen, die auf die URL zugreifen kann.)

Die Xerox® Device Management-Anwendungen werden als Hintergrundprozess mittels lokaler Systemkontoberechtigungen ausgeführt, um die Netzwerkdruckgeräte automatisch via SNMP abzufragen und die Attribute der Druckgeräte regelmäßig an die Xerox Communication Server zu übertragen.

Zugriff auf die Benutzeroberflächen (UI) der Xerox® Device Manager (XDM)-Anwendung und deren Funktionen werden über die folgenden rollenbasierten Berechtigungen gesteuert (z. B. Centre Ware® Web-Administratoren, Centre Ware® Web Power-Benutzer, Centre Ware® Web SQL-Benutzer, Centre Ware® Web-Kundenadministratoren und benannte Centre Ware® Web-Kundengruppen).

Benutzernamen und Kennwörter für die Anwendungen werden nicht im Netzwerk versendet. Stattdessen werden Zugriffs-Token verwendet (gemäß des Designs des Windows® Betriebssystems)

Die Xerox® Device Manager (XDM)-Anwendung stellt Sicherheit basierend auf der Steuerung der Druckauftragsabsetzung zur Verfügung, indem sie Aufträge basierend auf der Richtlinie zur Farbnutzung, Dokumentenart, Auftragskosten, Tageszeit, Zugriffssteuerung für Benutzergruppen, Duplex-Richtlinie, erlaubte Auftragsdruckausgaben und aufgrund von Druckkontingenten einschränkt.

Hinweis: Die Nutzung von SNMP durch eine Xerox® Remote Services-Anwendung sollte kein Sicherheitsrisiko für die Kunden-IT-Umgebung darstellen, weil der gesamte auf SNMP basierende oder von diesen Anwendungen verbrauchte Verkehr innerhalb des Kunden-Intranets, hinter der Firewall stattfindet. Der Windows SNMP-Dienst und der Windows SNMP Trap-Dienst werden nicht standardmäßig im Windows-Betriebssystem aktiviert.

Unternehmenssicherheitsmodus

Zusätzlich zu geplanten Synchronisationen durch die Xerox® Device Management-Anwendungen zum Xerox® Services Manager wird standardmäßig eine tägliche Synchronisation durchgeführt. Die beiden Unternehmenssicherheitsmodi sind **Normal-** und **Sperrmodus (Lock Down).**

In **Normal**-Modus kontaktiert die Device Management-Anwendung den Xerox® Services Manager täglich, wenn alle anderen geplanten Synchronisationen ausgeschaltet sind ***(Empfohlener Modus***).

Im **Sperrmodus** gibt es außer druckerbezogener Datensynchronisation keine Kommunikation mit Xerox® Services Manager. Änderungen an dieser Einstellung müssen vor Ort vorgenommen werden. (***Datensynchronisierung*** sorgt dafür, dass die Druckgeräteinformationen, die von der Xerox® Device Management-Anwendung gesendet werden, mit den im Xerox® Services Manager aufgenommenen Informationen übereinstimmen.)

Standardmäßig wird der Xerox® Services Manager täglich von der Xerox® Device Management-Anwendung kontaktiert und Administratoren können Einstellungen entfernt ändern, was einen Kundendienstbesuch vor Ort vermeidet. Wir empfehlen diese Einstellung nicht zu verändern. Wenn ein Kunde den Support der Druckgeräte durch das Xerox-Personal einschränkt, kann die Gerätekommunikation zu Xerox® Services Manager bis auf die Druckerdatensynchronisation gesperrt werden. In diesem Modus berichtet die Anwendung keine Computer- oder Drucker-IP-Adressen oder Standorteinstellungen an Xerox® Services Manager und alle Einstellungsänderungen müssen vor Ort vorgenommen werden.

Hinweis: Wenn Xerox® Device Agent nicht das Register „Unternehmenssicherheitsmodus“ enthält, arbeitet das Programm im Normalmodus.

Protokolle, Ports und andere verwandte Technologien

Die folgende Tabelle identifiziert die Protokolle, Ports und Technologien, die innerhalb der Xerox® Remote Services verwendet werden:

Portnummer	Protokoll	Beschreibung der Verwendung	Datenfluss im Netzwerk
Abhängig von den Protokollen der oberen Schichten	**Internet Protocol (IP)**	**Zugrundeliegender Transport für alle Datenkommunikationen**	**Intern + Extern (nur ausgehend)**
Nicht verfügbar	Internet Control Message Protocol (ICMP)	Erkennung und Fehlerbeseitigung für Druckgeräte	Intern
25	Simple Mail Transport Protocol (SMTP)	Druckgerät + Remote Proxy App - E-Mail-Benachrichtigungen	Intern
53	Domain Name Services (DNS)	Wird für auf DNS basierende Erkennungsprozesse von Druckgeräten verwendet	Intern
80	HyperText Transport Protocol (HTTP)	Abfragen der Druckgeräte-Webseite + Abfragen der Device Management-Anwendungswebseite	Intern
135	Remote Procedure Call (RPC)	Erkennung von Druckgeräten	Intern
137, 139	NetBIOS	Druckserverfeststellung	Intern

Portnummer	Protokoll	Beschreibung der Verwendung	Datenfluss im Netzwerk
161	Simple Network Management Protocol (SNMP V1 / V2C / V3)	Industriestandardprotokoll, das bei der Erkennung von vernetzten Druckgeräten verwendet wird + Abholen von Status-, Zähler- und Verbrauchsmaterialiendaten + Abholen und Anwenden von Druckgerätekonfigurationen. Standardmäßige Community-Namen = “public” (GET), “private” (SET)	Intern
162	SNMP-Traps	Standardmäßiger Community-Name = “SNMP_trap”	Intern
389	Lightweight Direct Access Protocol (LDAP)	Erkennung von Druckgeräten via MS Active Directory Partitionsaufzählung + Konfigurationssatz für Scan-Dienste + Kundenimport in Active Directory + Kundengruppenkonfigurationen	Intern
443	Sicheres HyperText Transport Protocol (HTTPS)	Abfragen der sicheren Druckgerät-Webseite (falls konfiguriert) + Abfragen der sicheren Remote Proxy App-Webseite (falls konfiguriert) + Druckgerät-Datentransfer zurück zu den Xerox® Communication Servern + Drucksteuerungskommunikationen zurück zu Xerox® Device Manager	Intern + Extern (nur ausgehend)
452	Netware Service Advertising Protocol (SAP)	Erkennung von Druckgeräten mittel Novell-Serverabfragen via IPX	Intern
515, 9100, 2000, 2105	Absetzen von Druckaufträgen via TCP/IP LPR & Raw Port	Softwareaktualisierungen auf Druckgeräten + Diagnose mittels Drucken von Testseiten	Intern
631	Internet Printing Protocol (IPP)	Erkennung von Druckgeräten	Intern

Beste Sicherheitsverfahren

Stellen Sie sicher, dass immer die neuesten Firmware- und Softwareversionen auf den Druckgeräten installiert sind. Verwenden Sie entweder die Web-Benutzeroberfläche (UI) des Druckgeräts oder die von Xerox® und anderen Druckeranbietern zur Verfügung gestellte Druckerverwaltungs-Anwendung, um die Firmware/Software des Druckgeräts zu aktualisieren.

Wenn möglich, deaktivieren Sie nicht verwendete Ports und Protokolle des Druckgeräts. Dies wird typischerweise auf der Web-Benutzeroberfläche (UI) von Bürodruckgeräten und auf der lokalen Benutzeroberfläche (UI) von Produktionsdruckgeräten durchgeführt.

Falls verfügbar, verwenden Sie die für die Benutzerzugriffsteuerung relevanten Funktionen der Druckgeräte. Dies wird typischerweise auf der Web-Benutzeroberfläche (UI) von Bürodruckgeräten und auf der lokalen Benutzeroberfläche (UI) von Produktionsdruckgeräten durchgeführt.

Wenn möglich, verwenden Sie sichere Protokolle. Dies wird typischerweise auf der Web-Benutzeroberfläche (UI) von Bürodruckgeräten und auf der lokalen Benutzeroberfläche (UI) von Produktionsdruckgeräten durchgeführt.

Aktivieren Sie die in dem Gerät eingebetteten Sicherheitsfunktionen (z.B. Überschreiben des Bildes, Festplattenverschlüsselung, sicheres Drucken usw.).

Stellen Sie sicher, dass die Unternehmens-Firewall in Übereinstimmung mit den Firmenrichtlinien zur Sicherheit HTTPS-Pakete über Port 443 leiten kann.