

VERSIE 7.0.0
MEI 2023
702P08992

Xerox[®] FreeFlow[®] Core

Beveiligingshandleiding

© 2023 Xerox Corporation. Alle rechten voorbehouden. Xerox® en FreeFlow® zijn handelsmerken van Xerox Corporation in de Verenigde Staten en/of andere landen.

Deze software omvat software die is ontwikkeld door Adobe Systems Incorporated.

Adobe, het Adobe-logo, het Adobe PDF-logo, PDF Converter SDK, Adobe Acrobat Pro DC, Adobe Reader DC en PDF Library zijn geregistreerde handelsmerken of handelsmerken van Adobe Systems Incorporated in de Verenigde Staten en/of andere landen.

Google Chrome™ browser is een handelsmerk van Google LLC.

Microsoft®, Windows®, Edge®, Microsoft Language Pack, Microsoft Office 2016, Microsoft Office 2019, Microsoft Office 2021, Microsoft Office 365, Microsoft SQL Server en Internet Explorer® zijn geregistreerde handelsmerken van Microsoft Corporation in de Verenigde Staten en/of andere landen.

Apple®, Macintosh®, Mac®, Mac OS® en Safari® zijn handelsmerken of geregistreerde handelsmerken van Apple Inc., geregistreerd in de Verenigde Staten en/of andere landen.

Mozilla Firefox is een handelsmerk van Mozilla Foundation in de V.S. en andere landen.

BR38371

Inhoudsopgave

Overzicht	5
Doel	6
Doelgroep	7
Disclaimer	8
Productbeschrijving.....	9
Structuur van de systeemsoftware	10
Beveiligingsaspecten van bepaalde functies	11
Systeemtoegang	12
Netwerkverbindingen.....	12
FIPS- en GDPR-compatibiliteit	23
Algemene bescherming van veiligheid	24
Bescherming van gebruikersgegevens	24
Toegang tot gebruikersaccount en opdrachten bewaren	25
Toegangscodes voor gebruikersaccounts	25
Gebruikersaccount vergrendelen	25
Gebruikersaccount afmelden.....	25
Activiteit van gebruikersaccount	25
Opdrachten bewaren	25
Opdrachteigenschappen	25
Rechten van gebruikersaccount	26
Beveiliging	27
Virusbeveiliging.....	28
Software-update	29
Aanvullende informatie en bronnen	31

Overzicht

Dit hoofdstuk bevat:

Doel.....	6
Doelgroep.....	7
Disclaimer.....	8

Doel

Het doel van deze beveiligingshandleiding is om informatie te verstrekken over de productbeveiliging van Xerox® FreeFlow® Core. In deze context wordt productbeveiliging gedefinieerd als de manier waarop gegevens worden opgeslagen en verzonden, hoe het product zich gedraagt in een netwerkomgeving, en hoe het product lokaal en extern toegankelijk is. Dit document beschrijft het ontwerp, de functies en toepassingen van Xerox® FreeFlow® Core met betrekking tot informatiezekerheid (IA) en de bescherming van klantgevoelige informatie.

Dit document biedt geen informatie voor zelfstudieprogramma's over de beveiliging en connectiviteit van Xerox® FreeFlow® Core-toepassingen en -functies. Voor meer informatie over deze toepassingen en functies raadpleegt u de *Xerox® FreeFlow® Core Help*. Verondersteld wordt dat de klant praktische kennis van deze onderwerpen heeft.

Klanten zijn verantwoordelijk voor de beveiliging van hun netwerk en het FreeFlow-product. Het FreeFlow-product legt geen beveiliging op in een netwerkomgeving.

Doelgroep

De doelgroep voor dit document zijn klanten die meer beveiligingsinformatie nodig hebben met betrekking tot de Xerox® FreeFlow® Core-software.

Disclaimer

De informatie in dit document is nauwkeurig op de datum van publicatie en wordt zonder garanties verstrekt. In geen geval kan Xerox® Corporation aansprakelijk worden gesteld voor enige schade die de gebruiker ondervindt als gevolg van het gebruiken dan wel het negeren van de informatie die in dit document wordt verstrekt, met inbegrip van directe of indirecte schade, incidentele schade, gevolgschade, winstderving of bijzondere schade, zelfs wanneer Xerox® Corporation van tevoren in kennis is gesteld dat dergelijke schade zou kunnen ontstaan.

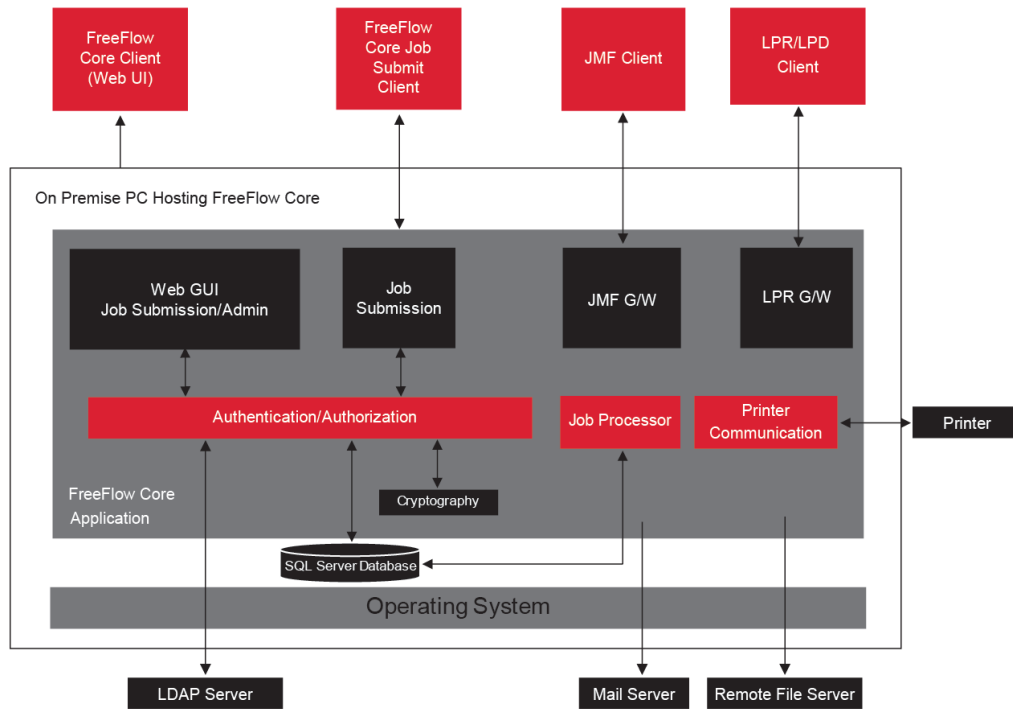
Productbeschrijving

Dit hoofdstuk bevat:

Structuur van de systeemsoftware 10

Xerox® FreeFlow® Core is de nieuwe generatie workflowoplossingen van Xerox. FreeFlow Core is een browser-gebaseerde oplossing waarmee de verwerking van afdrukopdrachten op intelligente wijze wordt geautomatiseerd en geïntegreerd, vanaf de voorbereiding van een bestand tot de eindproductie. Met FreeFlow Core beschikt u over een gebruikersvriendelijke workflow die u eenvoudig kunt bedienen, aanpassen en op schaal brengen en die consistente resultaten levert.

Structuur van de systeemsoftware



Beveiligingsaspecten van bepaalde functies

Dit hoofdstuk bevat:

Systeemtoegang	12
FIPS- en GDPR-compatibiliteit.....	23
Algemene bescherming van veiligheid.....	24
Toegang tot gebruikersaccount en opdrachten bewaren	25
Rechten van gebruikersaccount.....	26

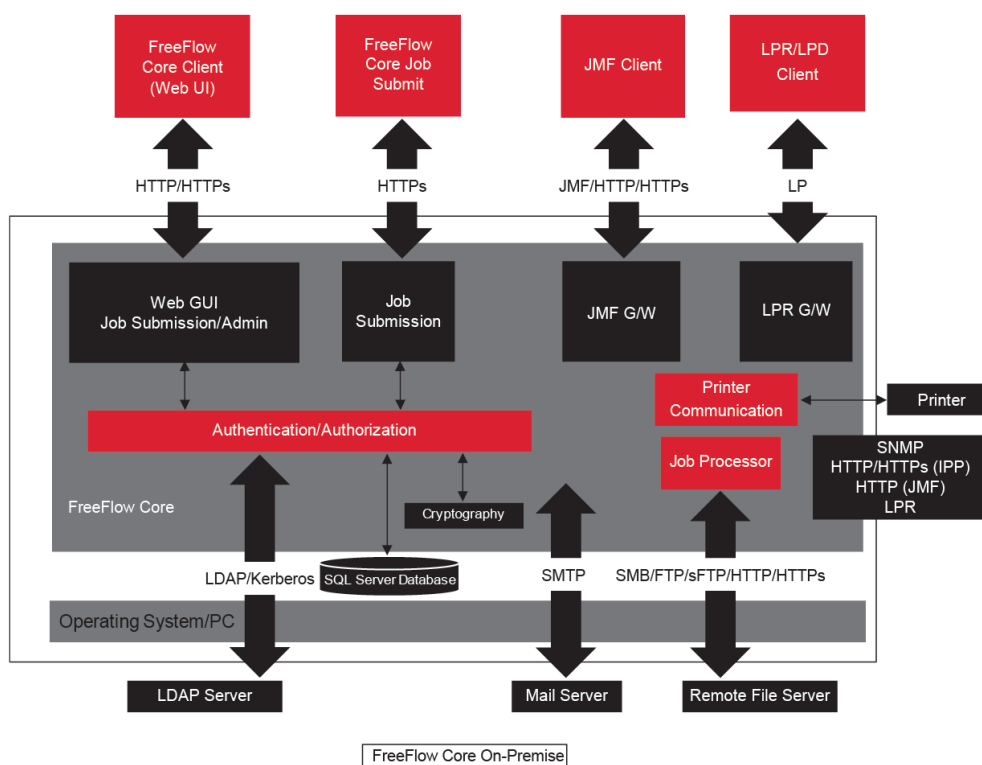
Systeemtoegang

NETWERKVERBINDINGEN

Xerox® FreeFlow® Core vereist een netwerkverbinding voor zowel opdrachtverwerking als gebruikersinteracties. Raadpleeg de beveiligingsinformatie voor elke netwerkverbinding.



 **Opmerking:** Voor een betere beveiliging en bescherming tegen aanvallen op zwakke plekken, schakelt u de Windows-firewall in op de server waarop FreeFlow Core is geïnstalleerd.

FreeFlow Core maakt gebruik van de volgende netwerkprotocolverbindingen.





Xerox® FreeFlow® Core-client

Voor de verbinding met FreeFlow Core is een webbrowser vereist die compatibel is met HTML5 en CSS3. Er zijn HTTPS-verbindingen vereist voor het beveiligd downloaden van de Xerox® FreeFlow® Core-client en beveiligde communicatie tussen de client en Xerox® FreeFlow® Core.

- Voeg een servercertificaat toe aan Internet Information Services (IIS) om HTTPS-verbindingen in te schakelen. Volg de instructies in de Windows-documentatie.
- Als HTTPS-verbindingen zijn ingeschakeld, moet u de instelling SSL vereisen in Microsoft Internet Information Services (IIS) instellen. Vanaf de Windows-opdrachtprompt voert u het batchbestand SSL vereisen uit. U vindt dit bestand in de directory met de naam Ondersteuning binnen de installatiedirectory van FreeFlow Core of in `C:\Program Files\Xerox\FreeFlow Core`.
- FreeFlow Core ondersteunt cryptografische TLS-protocollen.
 -  Opmerking: FreeFlow Core gebruikt de instellingen van het besturingssysteem die het TLS-protocol ondersteunen. Om te zorgen dat de huidige versies van de cryptografische protocollen worden gebruikt, wordt aangeraden om het besturingssysteem met de nieuwste updates te gebruiken.
- Er worden geen klantgegevens uitgewisseld tussen de client en de Xerox® FreeFlow® Core Server, tenzij gebruikers opdrachtbestanden downloaden.
 -  Opmerking: De client haalt de opdrachteigenschappen op waarin de klantgegevens zijn opgenomen.

Tabel 3.1 Configuratie van de firewall

POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
80	HTTP	Inkomend  Opmerking: Het poortnummer is afhankelijk van de configuratie van de IIS-server.
443	HTTPS	Inkomend  Opmerking: Het poortnummer is afhankelijk van de configuratie van de IIS-server.

Gebruikersrollen

Xerox® FreeFlow® Core wordt geopend met een aanmeldingsscherm.

- Gebruikers moeten zich aanmelden voor toegang tot het FreeFlow Core-systeem.
- Aangemelde gebruikers worden automatisch afgemeld als ze 30 minuten niet actief zijn geweest.
- Als de verificatie met de FreeFlow Core-software mislukt, wordt de applicatie na drie mislukte aanmeldingspogingen vergrendeld voor gebruikers.

 Opmerking: Raadpleeg [Toegang tot gebruikersaccount en opdrachten bewaren](#) voor aanvullende gebruikersaccountinstellingen. De FreeFlow Core-beheerder configureert de instellingen.

Voor het toewijzen van gebruikers aan gebruikersrollen raadpleegt u *Xerox® FreeFlow® Core Help, Instellingen gebruikerstoegang*.

Rol Beheerder

Beheerders hebben toegang tot het hele systeem:

- Functies op het tabblad Opdrachtbeheer en Opdrachtstatus: Dialoogvenster Opdracht verzenden en tabblad Opdrachtstatus.
- Tabbladen Printerbeheer en Printerstatus
- Instellingen workflow
- Functies op het tabblad Beheer:
 - Hot folder
 - Meldingen
 - Gebruikerstoegang
 - Land
 - Beveiliging
 - Core Rapporten
 - Core Exchange
 - Wachtrij-opties
 - Core-licentie
- Hulpprogramma's Core Server beschikbaar op bureaublad van server:
 - FreeFlow® Core Exchange
 - FreeFlow® Core Configureren
 - FreeFlow® Core Rapporten voor opdrachtregelhulpprogramma



Opmerking: Er kan slechts één beheerder tegelijk zijn aangemeld bij Xerox® FreeFlow® Core.

Rol Operateur

Operateurs hebben toegang tot:

- Functies op het tabblad Opdrachtbeheer en Opdrachtstatus: dialoogvenster Opdracht verzenden en tabblad Opdrachtstatus
- Tabbladen Printerbeheer en Printerstatus



Opmerking: Meerdere operateurs kunnen tegelijkertijd zijn aangemeld bij Xerox® FreeFlow® Core.

Rol Opdrachtstatusmonitor

De opdrachtstatusmonitor heeft alleen-lezen toegang tot het tabblad Opdrachtstatus.



Opmerking: Meerdere gebruikers die aan de rol Opdrachtstatusmonitor zijn toegewezen kunnen tegelijkertijd zijn aangemeld bij Xerox® FreeFlow® Core.




Gebruikersverificatie

De ingevoerde aanmeldingsgegevens in de Xerox® FreeFlow® Core-browserclient worden niet gecodeerd bij gebruik van HTTP. Voor beveiligde verzending schakelt u HTTPS en SSL vereisen bij IIS in voor beveiligde webtoegang tot Xerox® FreeFlow® Core.

- Bij verificatie van gebruikers via Xerox® FreeFlow® Core wordt de gebruikersinformatie niet gecodeerd. Aanmeldingsgegevens worden lokaal opgeslagen en gecodeerd.
- Bij verificatie van gebruikers via Active Directory worden de aanmeldingsgegevens niet gecodeerd voordat ze naar Active Directory worden verzonden. Bij verificatie via Active Directory worden de aanmeldingsgegevens niet lokaal opgeslagen.
- U kunt Xerox® FreeFlow® Core-verificatie instellen op het gebruik van een bestaande Windows Active Directory. Deze configuratie gebruikt de huidige aanmeldingsgegevens van de bureaubladgebruiker als de aanmeldingsgegevens voor de Xerox® FreeFlow® Core-client.

De verbinding van de Xerox® FreeFlow® Core-configuratie met Active Directory wordt gecodeerd voor de configuratie van het besturingssysteem.

Tabel 3.2 Configuratie van de firewall

POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
80	HTTP	Inkomend  Opmerking: Het poortnummer is afhankelijk van de configuratie van de IIS-server.
88	Kerberos	Uitgaand: Gebruikersverificatie  Opmerking: De poortnummers en services zijn afhankelijk van de AD-configuratie op de server.
389636 3268 3269	LDAP LDAP TLS LDAP GC LDAP GC TLS	Uitgaand: Valideert AD-groepen tijdens de configuratie van AD-verificatie  Opmerking: De poortnummers en services zijn afhankelijk van de AD-configuratie op de server.


SQL Server-verbinding

Xerox® FreeFlow® Core communiceert met de SQL Server met behulp van Entity Framework van Microsoft®. Gecodeerde communicatie tussen Xerox® FreeFlow® Core en de SQL Server wordt ingeschakeld wanneer de SQL Server is geconfigureerd voor het gebruik van gecodeerde verbindingen.

Gecodeerde aanmeldingsgegevens voor de SQL Server worden plaatselijk opgeslagen op de Xerox® FreeFlow® Core-server.

Om software te installeren op een externe SQL Server zonder SQLS-beheerdersrechten, maakt u twee lege databases in de SQLS-instantie:



- OapMasterDatabase
- OapPlatformDatabase

POOR- RT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
1433	SQLS	Inkomend: Ontvangt verbindingen van Xerox® FreeFlow® Core Uitgaand: Communiceert met de database-engine van SQL Server  Opmerking: Het poortnummer is afhankelijk van de configuratie van de SQLS-server.
1434	SQLS Browser-service	Inkomend: Ontvangt verbindingen van Xerox® FreeFlow® Core Uitgaand: Communiceert met de database-engine van SQL Server  Opmerking: De server biedt de client een poortnummer voor de verbinding.

Gebruikersinterface voor opdrachtverzending


De gebruikersinterface voor opdrachtverzending maakt gebruik van de Xerox® FreeFlow® Core Client-verbinding voor het verzenden van opdrachten. Raadpleeg [Xerox® FreeFlow® Core-client](#) voor meer informatie.

Tabel 3.3 Configuratie van de firewall

PO- ORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
80	HTTP	Inkomend  Opmerking: Het poortnummer is afhankelijk van de configuratie van de IIS-server.
443	HTTPS	Inkomend  Opmerking: Het poortnummer is afhankelijk van de configuratie van de IIS-server.

Hot folders

Gebruik bestandsshare om een lokale hot folder te delen en om toegang te krijgen tot een hot folder in gedeelde Windows-mappen. Gebruik het Windows-bestandssysteem om Windows-mappen te coderen. Gebruik Windows-toegangsbeheer van gebruikersaccounts om Windows-mappen te beveiligen.

-  Opmerking: Als u toegangsbeheer op gebruikersaccounts toepast, gebruik dan dezelfde serviceaccount die u hebt gebruikt in de configuratie van de *Optionele installatieprocedures*. Voor meer informatie raadpleegt u de *Xerox® FreeFlow® Core Installatiehandleiding*.

Tabel 3.4 Configuratie van de firewall


POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
139, 445	SMB	Inkomend: Deelt hot folders via Windows Bestanden delen Uitgaand: Gebruikt hot folders in gedeelde directory's
20, 21	FTP	Inkomend: Deelt hot folders via FTP

Manifestverwerking

Bij de verzending van het manifest haalt Xerox® FreeFlow® Core de bestanden op die in het manifest staan vermeld. U kunt naar de bestanden verwijzen met behulp van toegewezen stations, UNC-bestandspaden, HTTP, HTTPS, FTP of sFTP URI's.

 Opmerking: HTTP en FTP URI's ondersteunen geen codering.


Gebruik bestandsshare om een lokale hot folder te delen en om toegang te krijgen tot een hot folder in gedeelde Windows-mappen. Gebruik het Windows-bestandssysteem om Windows-mappen te coderen. Gebruik Windows-toegangsbeheer van gebruikersaccounts om Windows-mappen te beveiligen.

 Opmerking: Als u toegangsbeheer op gebruikersaccounts toepast, gebruik dan dezelfde serviceaccount die u hebt gebruikt voor de configuratie van de Optionele installatieprocedures. Voor de meeste recente instructies over het inschakelen van Office-conversie raadpleegt u de *Xerox® FreeFlow® Core Release-informatie*. Als u het document wilt hebben, gaat u naar de FreeFlow® Core-webpagina op <https://xerox.com/automate>. Klik bovenaan de pagina op **Owner Resources** (Hulpbronnen voor eigenaars) en klik dan op **Release Notes** (Release-informatie), waarbij de volledige systeemvereisten zijn inbegrepen.

Tabel 3.5 Configuratie van de firewall

POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
139, 145	SMB	Uitgaand: Haalt bestanden op die in het manifest staan vermeld uit gedeelde directory's
20, 21	FTP	Uitgaand: Haalt bestanden op die in het manifest staan vermeld
80	HTTP	Uitgaand: Haalt bestanden op die in het manifest staan vermeld
443	HTTPS	Uitgaand: Haalt bestanden op via de HTTPS URL die in het manifest staat vermeld
22	sFTP	Uitgaand: Haalt bestanden op via de beveiligde FTP die in het manifest staat vermeld

Line Printer Daemon (LPD)


 Opmerking: Line Printer-commando's (LP) ondersteunen geen beveiligde verbindingen.

Tabel 3.6 Configuratie van de firewall

POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
515	LP	Inkomend: Ontvangt LPR-verzoeken (Line Printer Remote) en LP-commando's
721 tot 731	LPR	Uitgaand: Verzendt LPR-verzoeken naar een printer die LPD ondersteunt.

JMF-commando's en printerstatussignalen


Job Messaging Format (JMF)-opdrachten en signalen aan een JMF-client ondersteunen beveiligde verbindingen. Het ophalen van JMF-bestanden ondersteunt HTTPS-verbindingen.

 Opmerking: Om JMF-verzendingen te beveiligen, verzendt u een MIME-pakket met de JMF-, JDF- en PDF-bestanden.

HTTPS-communicatie inschakelen voor JMF-commando's:

1. Om een certificaat aan de Java-keystore toe te voegen, gebruikt u het hulpprogramma `installJMFCertificate.bat` in de Xerox® FreeFlow® Core-installatiedirectory.
2. Start de Xerox® FreeFlow® Core JMF Server-service opnieuw.
3. Om de installatie te testen, gaat u naar `http://<hostnaam>:7759/FreeFlowCore`. Als beveiligde JMF juist is geconfigureerd, wordt een HTTP Status 404-foutpagina weergegeven in de browser.

Tabel 3.7 Configuratie van de firewall


POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
7751	JMF	Inkomend: Ontvangt JMF-commando's
Varieert	JMF	Uitgaand: Retourneert JMF-printerstatussignalen  Opmerking: De client die de JMF-printerstatussignalen of het JMF-retoursignaal aanvraagt, definieert het vereiste poortnummer.
7759	sJMF	Inkomend: Ontvangt beveiligde JMF-commando's

Knooppunten in de workflow

Workflowcomponenten die opdrachtbestanden ophalen of opslaan kunnen toegewezen stations, UNC-bestandspaden, HTTP, HTTPS of FTP URI's gebruiken. sFTP URI ondersteunt het ophalen van opdrachtbestanden zoals MAX, JMF.

 Opmerking: HTTP en FTP URI's ondersteunen geen codering.

Gebruik het Windows-bestandssysteem om bestandsshare te coderen voor het delen. Gebruik Windows-toegangsbeheer voor gebruikersaccounts om bestandsshare te beveiligen.

 Opmerking: When you use the user account access control, use the same service account that you used in the *Optional Installation Procedures* configuration. For more information, refer to the *Xerox® FreeFlow® Core Installation Guide*.

Tabel 3.8 Configuratie van de firewall

POO-RT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
139, 445	SMB	Inkomend: Haalt bestanden op die in een voorinstelling van de workflowcomponent worden gespecificeerd Uitgaand: Slaat bestanden op in gedeelde directory's
20, 21	FTP	Uitgaand: Haalt bestanden op die in een voorinstelling van de workflowcomponent worden gespecificeerd
80	HTTP	Uitgaand: Haalt bestanden op die in een voorinstelling van de workflowcomponent worden gespecificeerd
443	HTTPS	Uitgaand: Haalt bestanden op die in een voorinstelling van de workflowcomponent worden gespecificeerd

Xerox® FreeFlow® Core Printing

Xerox® FreeFlow® Core gebruikt SNMP en HTTP met IPP-, JMF- of XBDS-commando's voor het bepalen van het DFE-type (Digital Front End) via een ongecodeerde verbinding. Voor de SNMP-openbare communitytekenreeks op de printer of de DFE is de standaardinstelling vereist. Als de standaardinstelling van de SNMP-openbare communitytekenreeks op de printer of de DFE is gewijzigd, controleert u of de bijgewerkte instelling is geregistreerd met FreeFlow Core. Zorg dat alle printers die met FreeFlow Core zijn geregistreerd, dezelfde SNMP-openbare communitytekenreeks hebben. Voor instructies over het bijwerken van de SNMP-openbare communitytekenreeks raadpleegt u de release-informatie van Xerox FreeFlow Core.

De volgende bewerkingen maken gebruik van een ongecodeerde verbinding:

- Het ophalen van de lijst met DFE-wachtrijen.
- Het ophalen van de lijst met virtuele printers op de EFI DFE.
- Het ophalen van de printermogelijkheden.
- Opdrachtbewerkingen op de DFE.

- Het ophalen van informatie over opdrachtaccountadministratie. Deze bewerking is niet van toepassing op JMG.
- Verzending van een afdrukopdracht naar een printer via LPR.

Bij een verbinding met een DFE die is geconfigureerd voor ondersteuning van beveiligde IPP, wordt het verzenden van afdrukopdrachten gecodeerd. Om beveiligde IPP in te schakelen, gebruikt u de optie Beveiligd afdrukken bij de configuratie van de printerbestemming. Tussen FreeFlow Core en de DFE wordt TLS en SHA256-codering gebruikt.

Afdrukverzending via beveiligde IPP naar de FreeFlow Print Server inschakelen

Om afdrukverzending via beveiligde IPP naar de FreeFlow Print Server in te schakelen, gaat u als volgt te werk:

1. Voeg een TLS-certificaat toe aan de FreeFlow Print Server.
2. Selecteer **TLS inschakelen** in de instellingen van de Xerox® FreeFlow® Print Server.
3. Gebruik het Xerox® FreeFlow® Core-certificaat om het TLS-certificaat van de FreeFlow Print Server op te halen.



Opmerking: After successful secure IPP configuration, Certificate installed successfully message appears.

Afdrukverzending via beveiligde IPP naar de Fiery inschakelen

Om afdrukverzending via beveiligde IPP naar Fiery in te schakelen, gaat u als volgt te werk:

1. Om de gebruikersinterface van Fiery te starten, voert u het Fiery -IP-adres in een webbrowser in.
2. Selecteer **Fiery Configure** (Fiery configureren) in het linkervenster.
3. Meld u aan met de aanmeldgegevens van de Fiery-controller.
4. Selecteer **Security** (Beveiliging) en maak vervolgens een zelfondertekend certificaat of vul de gegevens van CA-certificaten in.
5. Schakel **SSL/TLS** op het configuratiescherm van de gebruikersinterface in.
6. Als SSL/TLS is ingeschakeld, verschijnt er een bevestigingsbericht dat u de controller opnieuw moet starten.
7. Selecteer **Yes** (Ja).
8. Start het **Windows-hulpprogramma Core Configureren** in Xerox® FreeFlow® Core.
9. Selecteer het tabblad **Core-certificaat**, voer het IP-adres van de Fiery-controller in en selecteer **Certificaat ophalen**.

Het bericht *Certificaat is geïnstalleerd* verschijnt.

10. Configureer de printer in Xerox® FreeFlow® Core met de beveiligde afdrukoptie op het scherm Printerbeheer.

Xerox® FreeFlow® Core ondersteunt geen communicatie met de DFE via beveiligde JMF.

Tabel 3.9 Configuratie van de firewall


POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
161, 162	SNMP v1/v2	Uitgaand: Identificeert het DFE-type tijdens de configuratie van de printerbestemming en het ophalen van het certificaat
80	HTTP	Inkomend: JDF-printer haalt het afdrukbestand via HTTP. Uitgaand: Identificeert het DFE-type tijdens de configuratie van de printerbestemming en het ophalen van het certificaat
N.V.T.	ICMP	Uitgaand: Controleert de beschikbaarheid van het apparaat voordat het certificaat wordt opgehaald
631	IPP v1.0/v1.1	Uitgaand: Verzendt opdrachten naar DFE's, haalt de opdrachtstatus op en verzendt opdrachtcommando's naar de DFE
4004	JMF	Inkomend: Ontvangt het bericht <code>JMF ReturnQueueEntry</code> van de printer
8010 of printer-gedefinieerde JMF-poort	JMF v1.3/v1.4	Uitgaand: Identificeert het DFE-type tijdens de registratie van de printer en verzendt een opdracht naar de DFE.
443	HTTPS	Uitgaand: Printercommunicatie met de DFE
515, 721 t/m 731	LPR	Uitgaand: Verzendt LPR-verzoeken naar een printer die LPD ondersteunt

E-mailmeldingen

Xerox® FreeFlow® Core is een e-mailclient die verbinding maakt met een toegankelijke SMTP-e-mailserver of een e-mailserver van Xerox. U kunt e-mailmeldingen coderen en daarna verbinding maken met een mailserver die codering ondersteunt. TLS maakt gecodeerde communicatie mogelijk tussen de meldingsservice en de SMTP-server.

Gecodeerde aanmeldingsgegevens worden lokaal opgeslagen.

Tabel 3.10 Configuratie van de firewall

POORT	PROTOCOL OF APPLICATIE	FIREWALL-VERBINDINGSTYPE
25, 465, 587	SMTP	Uitgaand: Verzendt e-mailmeldingen  Opmerking: Het vereiste poortnummer en gebruik van de beveiligde verbinding zijn afhankelijk van de configuratie van de SMTP-server.

FIPS- en GDPR-compatibiliteit

Xerox® FreeFlow® Core werkt op een Windows-besturingssysteem dat is ingeschakeld voor naleving van FIPS 140-2. Raadpleeg de Microsoft-documentatie voor het inschakelen van FIPS-compatibiliteit. FreeFlow Core werkt standaard in de FIPS-nalevingsmodus.

FreeFlow Core schakelt de ondersteuning voor DES/3DES-ciphers uit.

Als beveiligd afdrukken via IPP met samenvattingsverificatie is vereist, schakelt u de FIPS-nalevingsmodus uit. Hiermee is FreeFlow Core niet langer compatibel met de cryptografische vereisten.

FreeFlow Core is compatibel met de Europese Algemene Verordening Gegevensbescherming (AVG).

Algemene bescherming van veiligheid

BESCHERMING VAN GEBRUIKERSGEGEVENS

Document- en bestandsbeveiliging

FreeFlow Core codeert bestanden die zijn verzonden voor verwerking niet expliciet, voordat het bestand op het bestandssysteem van de pc wordt opgeslagen.

De broninhoud van documenten bevat persoonlijk identificeerbare informatie (PII) of andere gevoelige inhoud. Derhalve is de gebruiker verantwoordelijk voor het juiste gebruik van de digitale informatie in overeenstemming met de beste praktijk ter bescherming van informatie.

Persoonlijk identificeerbare informatie (PII)

Als u zich registreert voor een FreeFlow Core-softwarelicentie, wordt er PII-informatie verzameld. De informatie omvat onder meer:

- Bedrijfsnaam
- Activeringsleutel en serienummer
- Host-ID/systeem-UUID
- Gebruikersnaam
- Adres (straat, woonplaats, provincie, postcode, land)
- E-mailadres (optioneel)

Deze informatie wordt beveiligd verzonden naar de Xerox-licentiehost.

PII-informatie, met name het e-mailadres van de gebruiker die wordt gebruikt voor herstel van de toegangscode, wordt opgeslagen op het FreeFlow Core-systeem. De informatie wordt gecodeerd.

Toegang tot gebruikersaccount en opdrachten bewaren

TOEGANGSCODES VOOR GEBRUIKERSACCOUNTS

Een toegangscode mag maximaal 10 keer opnieuw worden gebruikt. Het aantal keren dat een toegangscode opnieuw mag worden gebruikt, is configureerbaar.

GEBRUIKERSACCOUNT VERGRENDELEN

Als verificatie via Xerox FreeFlow Core Client mislukt, worden gebruikers na drie mislukte aanmeldingspogingen afgemeld en 30 minuten lang vergrendeld. Het aantal mislukte aanmeldingspogingen en de vergrendelingsperiode zijn configureerbaar.

GEBRUIKERSACCOUNT AFMELDEN

Na 30 minuten inactiviteit worden aangemelde gebruikers van Xerox® FreeFlow® Core Client automatisch afgemeld. De duur van deze inactiviteitsperiode is configureerbaar.

ACTIVITEIT VAN GEBRUIKERSACCOUNT

Het auditlog van gebruikersaanmeldingen bevindt zich in Windows Logboekinzage, in het gedeelte **Toepassing** van de map **Windows-logboeken**.

OPDRACHTEN BEWAREN

Nadat een opdracht is verwerkt, is de bewaarperiode voor opdrachten in FreeFlow Core 24 uur.

De FreeFlow Core-printer is geconfigureerd om de bewaarperiode te wijzigen voordat voltooide opdrachten automatisch worden verwijderd. Na 24 uur worden voltooide opdrachten door de FreeFlow Core-printer verwijderd.

Gebruik de FreeFlow Core-webgebruikersinterface om opdrachten handmatig te verwijderen.

OPDRACHTEIGENSCHAPPEN

Zorgt voor beperking tegen het downloaden van bestanden die in Opdrachteigenschappen worden gevonden voor een opdracht die in FreeFlow Core Opdrachtbeheer en status wordt weergegeven.

Rechten van gebruikersaccount

Voor het configureren van de Xerox® FreeFlow® Core-serviceaccount kunt u een lokale beheerdersaccount of een niet-beheerdersaccount gebruiken. Als u een account gebruikt die lid is van de lokale beheerdersgroep, zijn geen speciale stappen vereist.

Als u een niet-beheerdersaccount gebruikt, zijn er aanvullende rechten nodig naast de standaardrechten van de gebruikersgroep. Met FreeFlow® Core Configureren worden automatische aanvullende rechten toegevoegd, zoals weergegeven in de onderstaande tabel:

INSTELLING GROEPSBELEID	NAAM VAN CONSTATE
Fungeren als deel van besturingssysteem	SeTcbPrivilege
Geheugentoe wijzingen voor een proces aanpassen	SeIncreaseQuotaPrivilege
Lokale aanmelding toestaan	SeInteractiveLogonRight
Back-up maken van bestanden en directory's	SeBackupPrivilege
Een token-object maken	SeCreateTokenPrivilege
Algemene objecten maken	SeCreateGlobalPrivilege
Permanente gedeelde objecten maken	SeCreatePermanentPrivilege
Debug van programma's	SeDebugPrivilege
Apparaatdrivers laden en verwijderen	SeLoadDriverPrivilege
Aanmelden als batchopdracht	SeBatchLogonRight
Aanmelden als service	SeServiceLogonRight
Audit- en beveiligingslog beheren	SeSecurityPrivilege
Vele onderhoudstaken uitvoeren	SeManageVolumePrivilege
Enkel proces profileren	SeProfileSingleProcessPrivilege
Systeemprestaties profileren	SeSystemProfilePrivilege
Token op procesniveau vervangen	SeAssignPrimaryTokenPrivilege



Opmerking: De rechten die in de tabel staan vermeld, zijn gedefinieerd in <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-rights-assignment>.

Beveiliging

Dit hoofdstuk bevat:

Virusbeveiliging.....28

Xerox neemt beveiligingskwesties uiterst serieus. Als vooraanstaand bedrijf in de ontwikkeling van digitale technologie verplicht Xerox zich ertoe digitale gegevens te beveiligen door potentiële zwakke plekken op te sporen en deze te verhelpen om risico's te beperken.

Xerox streeft ernaar de best beveiligde softwareproducten te leveren op basis van de informatie en technologie die op dit moment beschikbaar zijn en tegelijkertijd de prestaties, waarde, functionaliteit en productiviteit van de apparaten te handhaven.

Er wordt getest of de onderdelen van Xerox® FreeFlow® Core voldoen aan de beveiligingseisen met behulp van commercieel verkrijgbare scanprogramma's voor controle op kwetsbaarheid en penetratie. Kwetsbare plekken in toepassingen worden aangepakt aan de hand van de resultaten van Xerox-scans.

Xerox verspreidt beveiligingsbulletins wanneer dat nodig is. Informatie in beveiligingsbulletins wordt beschikbaar gesteld op de Xerox-beveiligingswebsite op <https://www.xerox.com/security>, bij Product Security Guidance. De website bevat de up-to-date printerstatus van kwetsbaarheden in de beveiliging, whitepapers, Common Criteria-certificering, Informatie van Intel Security McAfee en een portal om vragen over beveiliging bij Xerox in te dienen.

Virusbeveiliging

Xerox neemt speciale voorzorgsmaatregelen om er zeker van te zijn dat de Xerox-software virusvrij wordt verstuurd. Xerox adviseert om anti-virusdetectie en bescherming tegen eindpuntaanvallen te installeren op de FreeFlow Core Server. Deze software en het besturingssysteem worden up-to-date gehouden met de nieuwste beveiligingspatches zoals geadviseerd door de respectievelijke leveranciers.

Ter verbetering van de prestaties raden we u aan om de installatiedirectory's van Xerox® FreeFlow® Core en de MS SQL-server uit te sluiten van scans door de antivirussoftware.

U kunt de volgende bestanden uitsluiten van scans door de antivirussoftware:

- <FreeFlow Core-installatiedirectory>\Logs
- <FreeFlow Core-installatiedirectory>\Platform\Logs
- <FreeFlow Core-installatiedirectory>\JobSubmit\Logs
- <FreeFlow Core-installatiedirectory>\Config
- <FreeFlow Core-installatiedirectory>\Platform\Config
- <FreeFlow Core-gebruikersgegevensdirectory>\
- Mappen buiten de FreeFlow Core-gebruikersgegevensdirectory die door FreeFlow Core worden gebruikt

Software-update

Xerox is niet verantwoordelijk voor de status van het besturingssysteem waarop Xerox® FreeFlow® Core wordt uitgevoerd. Het is de verantwoordelijkheid van de klant om het systeem up-to-date te houden en om te zorgen dat de juiste patches zijn uitgevoerd en dat het systeem juist is geconfigureerd. Voer minstens een keer per maand een Microsoft® Windows®-update uit.

Als u de Windows-updates uitvoert, kunt u de update toepassen met behulp van de optie **Windows Update**. We raden aan om geen optionele preview-updates te installeren, omdat deze de betrouwbaarheid van de Xerox® FreeFlow® Core-server kunnen beïnvloeden.

U kunt software-updates voor FreeFlow Core vinden op <https://www.support.xerox.com/support/core/software/enus.html>. Klanten kunnen de software-update installeren.

Software-update

Aanvullende informatie en bronnen

Beveiliging @ Xerox

Xerox onderhoudt een actuele openbare website met de nieuwe beveiligingsinformatie met betrekking tot haar producten. Raadpleeg www.xerox.com/security.

Reacties op bekende zwakke plekken

Xerox heeft een document opgesteld met daarin uitleg over het Xerox-beleid omtrent beheer van zwakke plekken en openbaarmaking, dat wordt gebruikt bij het detecteren en herstellen van zwakke plekken in Xerox-software en -hardware. U kunt dit document op de volgende pagina downloaden: <https://www.xerox.com/information-security/information-security-articles-whitepapers/enus.html>.

Aanvullende bronnen

BEVEILIGINGSBRON	URL
Veelgestelde vragen over beveiliging	www.xerox.com/en-us/information-security/frequently-asked-questions
Bulletins, adviezen en beveiligingsupdates	www.xerox.com/security
Nieuwsarchief beveiliging	security.business.xerox.com/en-us/news/

