# GIDS VOOR MFD HARDENING

imageRUNNER ADVANCE

Canon

# INLEIDING

Moderne multifunctionele Canon-apparaten (MFD's) met functies als printen, kopiëren, scannen, verzenden en faxen. MFD's zijn volwaardige computerservers, die een aantal netwerkgeïntegreerde diensten in combinatie met een harde schijf met een aanzienlijk opslagruimte bieden.

Wanneer een organisatie deze apparaten in hun infrastructuur introduceert, zijn er een aantal gebieden die moeten worden aangepakt als onderdeel van de bredere beveiligingsstrategie, die moet toezien op de bescherming van de vertrouwelijkheid, integriteit en beschikbaarheid van uw netwerksystemen.

Natuurlijk zal de implementatie hiervan verschillen en zullen organisaties hun eigen specifieke beveiligingsvereisten hebben. Terwijl Canon samenwerkt om ervoor te zorgen dat Canon-apparaten worden geleverd met de juiste initiële beveiligingsinstellingen, wil Canon dit verder ondersteunen door een aantal configuratie-instellingen aan te bieden, waarmee u het apparaat beter op de vereisten voor uw specifieke situatie kunt afstemmen.

Dit document is ontworpen om voldoende informatie te verstrekken, zodat u de meest geschikte instellingen voor uw omgeving met Canon of een Canon-partner kunt bespreken. Houd er rekening mee dat niet alle hardware van het apparaat dezelfde capaciteit heeft en dat verschillende systeemsoftware mogelijk andere functionaliteit biedt. Nadat er hierover een besluit genomen is, kan de definitieve configuratie voor uw apparaat of apparatenpark worden toegepast. Voor meer informatie en ondersteuning kunt u contact opnemen met Canon of een Canon-partner.

### Voor wie is dit document bedoeld?

Dit document is gericht op iedereen die zich bezighoudt met het ontwerp, de implementatie en de beveiliging van multifunctionele kantoorapparaten (MFD's) binnen een netwerkinfrastructuur. Dit zijn bijvoorbeeld IT- en netwerkspecialisten, IT-beveiligingsprofessionals en servicepersoneel.

### Toepassing en bereik

In de gids wordt uitgelegd en advies gegeven over de configuratie-instellingen voor twee typische netwerkomgevingen, zodat organisaties op basis van best practice veilig een MFD-oplossing kunnen implementeren. Verder wordt (vanaf systeemsoftwareversie 3.8) uitgelegd hoe Syslog-functionaliteit real-time feedback van het MFD kan leveren. Deze instellingen zijn getest en gevalideerd door het beveiligingsteam van Canon.

Canon maakt geen veronderstellingen over specifieke regelgevende vereisten in de branche die andere beveiligingsoverwegingen kunnen opleggen en buiten het bereik van dit document vallen.

Deze gids is gemaakt op basis van de typische reeks eigenschappen van het imageRUNNER ADVANCE-platform, en terwijl de informatie hierin voor alle modellen en series binnen het bereik van de imageRUNNER ADVANCE-reeks geldt, kunnen sommige functies tussen de modellen verschillen.

### Implementatie van passende MFD-beveiliging voor uw omgeving

Om de beveiligingsimplicaties van een multifunctioneel apparaat als onderdeel van uw netwerk te onderzoeken, heeft Canon twee typische scenario's overwogen:

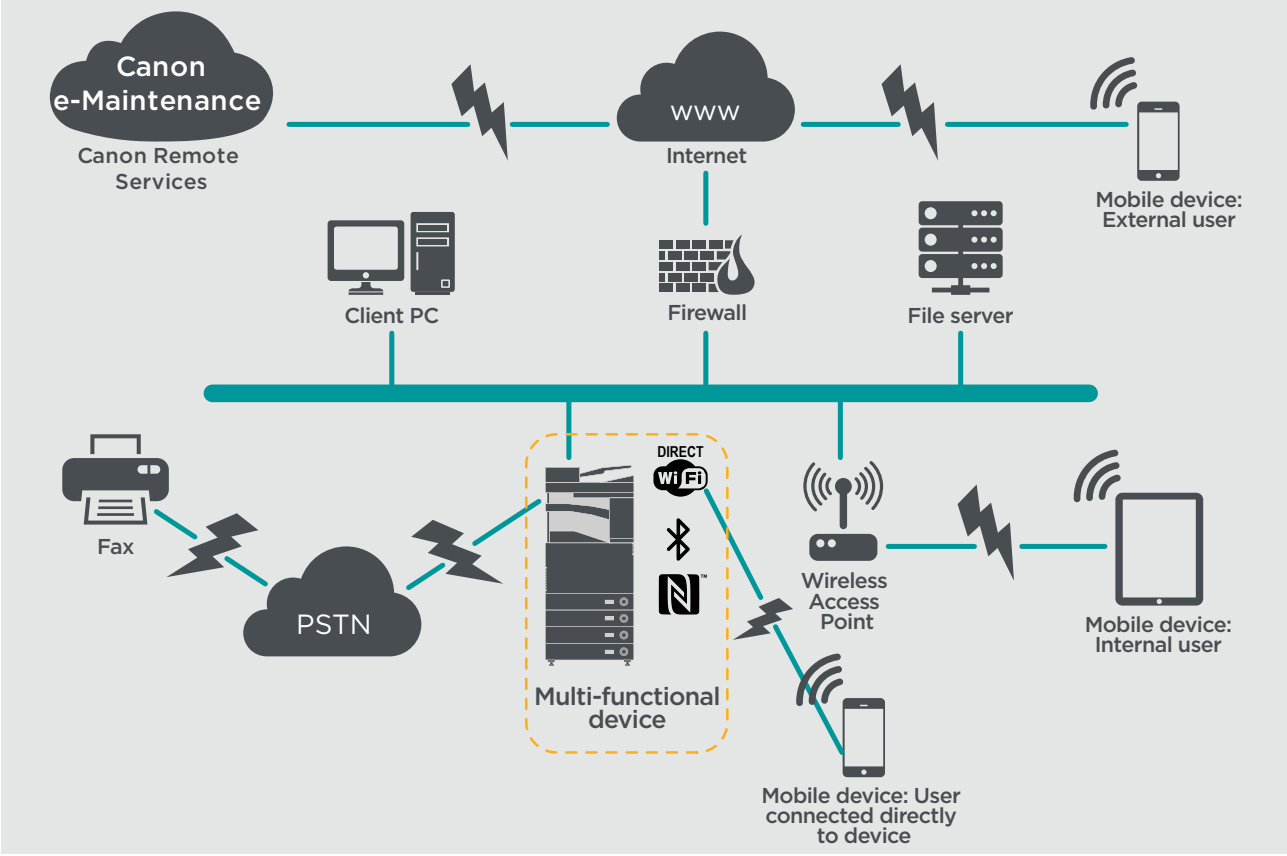
- **Een typische kleine kantooromgeving**
- **Een kantooromgeving in een grote onderneming**

# KLEINE KANTOOROMGEVING

Dit is meestal een kleine bedrijfsomgeving met een ongesegmenteerde netwerktopologie. Hierin wordt gebruik gemaakt van een of twee MFD's voor intern gebruik en deze apparaten zijn niet toegankelijk via het internet.

Terwijl mobiel printen beschikbaar is, zijn er aanvullende oplossingscomponenten vereist. Voor die gebruikers die printerdiensten buiten een LAN-omgeving nodig hebben, is een beveiligde verbinding vereist, maar dit wordt niet in deze gids behandeld. Er moet echter aandacht uitgaan naar de beveiliging van de gegevens die worden uitgewisseld tussen het externe apparaat en de printinfrastructuur.

**Afbeelding 1** Klein kantoornetwerk




De nieuwste generatie van imageRUNNER ADVANCE-modellen bieden wireless netwerkconnectiviteit, waardoor het apparaat met een WiFi-netwerk verbonden kan worden. Het kan ook worden gebruikt om een point-to-point WiFi Direct-verbinding met een mobiel apparaat tot stand te brengen, zonder de noodzaak van een netwerkverbinding.

Voor diverse apparaatmodellen zijn Bluetooth- en NFC-opties beschikbaar, die alleen gebruikt worden voor het tot stand brengen van een WiFi Direct-verbinding voor iOS- en Android-apparaten.

# CONFIGURATIE-OVERWEGINGEN

Neem in acht dat, tenzij er hierna een functie van de imageRUNNER ADVANCE wordt vermeld, de standaardinstellingen voor dit bedrijf en deze netwerkomgeving als voldoende worden beschouwd.

**Tabel 1** Configuratie-overwegingen kleine kantooromgeving

| Functie imageRUNNER ADVANCE | Beschrijving | Overweging |
|---|---|---|
| Servicemodus | Voor toegang tot instellingen Servicemodus | Wachtwoordbeveiliging met een niet-standaard, niet-triviaal wachtwoord met een maximumlengte |
| Servicemanagement-systeem | Voor toegang tot diverse niet-standaard apparaatinstellingen | Wachtwoordbeveiliging met een niet-standaard, niet-triviaal wachtwoord met een maximumlengte |
| SMB bekijken/verzenden | Opslaan onder en opvragen vanuit Windows / SMB-netwerkshares | Systeembeheerders moeten, op basis van beleid, alle gebruikers verbieden lokale accounts op hun client-machine te creëren voor gebruik bij het het delen van documenten met de imageRUNNER ADVANCE via SMB |
| Externe gebruikersinterface | Web-based configuratietool | De imageRUNNER ADVANCE-beheerder moet HTTPS voor de externe gebruikersinterface inschakelen en HTTP-toegang uitschakelen. Inschakelen van gebruik van unieke PIN-verificatie voor elk apparaat |
| SNMP | Integratie netwerkcontrole | Versie 1 uitschakelen en versie 3 inschakelen |
| Naar e-mail en/of IFAX verzenden | E-mails met bijlagen vanaf apparaat verzenden | SSL inschakelen<br>Geen POP3-verificatie gebruiken voor verzenden SMTP<br>SMTP-verificatie gebruiken |
| POP3 | Automatisch documenten vanuit mailbox opvragen en printen | SSL inschakelen<br>POP3-verificatie inschakelen |
| Adresboek / LDAP | Directoryservice gebruiken voor het opzoeken van privénummer of e-mailadressen voor verzending van scans | SSL inschakelen<br>Geen domeingegevens voor verificatie met de LDAP-server gebruiken; LDAP-specifieke gegevens gebruiken |
| FTP-printen | Documenten naar en vanaf de embedded FTP-server uploaden en downloaden | Schakel FTP-verificatie in. Neem in acht dat FTP-verkeer altijd in leesbare tekst op het netwerk wordt verzonden |
| WebDAV verzenden | Documenten op een externe locatie scannen en opslaan | Verificatie voor WebDAV-shares inschakelen |
| Gecodeerde PDF | Documenten coderen | Op basis van beleid mogen vertrouwelijke documenten alleen<br>gecodeerd worden met behulp van PDF versie 1.6 (AES-128) |
| Secure Print | Printopdracht wordt naar het apparaat verzonden, maar in de printwachtrij geplaatst tot de bijbehorende PIN-code wordt ingevoerd | Met PIN-code beveiligde printopdrachten |
| Melding Syslog-gebeurtenis | Het System Logging Protocol is een standaardprotocol dat wordt gebruikt om systeemlog- of gebeurtenisberichten te verzenden naar een specifieke server die Syslog-server wordt genoemd | Overweeg de Syslog-gegevens van imageRUNNER te verwijzen naar uw bestaande Syslog-analysetool voor netwerken of naar het SIEM-platform (Security Event Management System) voor ondernemingen. |
| Verify-systeem bij het opstarten | Biedt de zekerheid dat de softwarecomponenten van het systeem niet in gevaar zijn gebracht. Dit heeft een minimale impact op de opstarttijd van het systeem | Functie activeren |
| Geïntegreerde webbrowser | Browsertoegang tot internet | Via beheer afdwingen van het gebruik van een inhoudfilterende webproxy om toegang tot schadelijke of virale inhoud te voorkomen. Creatie van favorieten uitschakelen |
| Bluetooth en NFC<br>(beschikbaar vanaf Generation 3-modellen) | Gebruikt voor het tot stand brengen van een WiFi Direct-verbinding | WiFi Direct inschakelen voor directe verbinding met een mobiel apparaat. WiFi Direct mag niet gebruikt worden wanneer WiFi wordt gebruikt om verbinding met een netwerk te maken |
| Draadloze LAN | Biedt wireless toegang | WPA-PSK/WPA2-PSK met sterke wachtwoorden gebruiken |
| IPP | Printopdrachten via IP verbinden en verzenden | IPP uitschakelen |

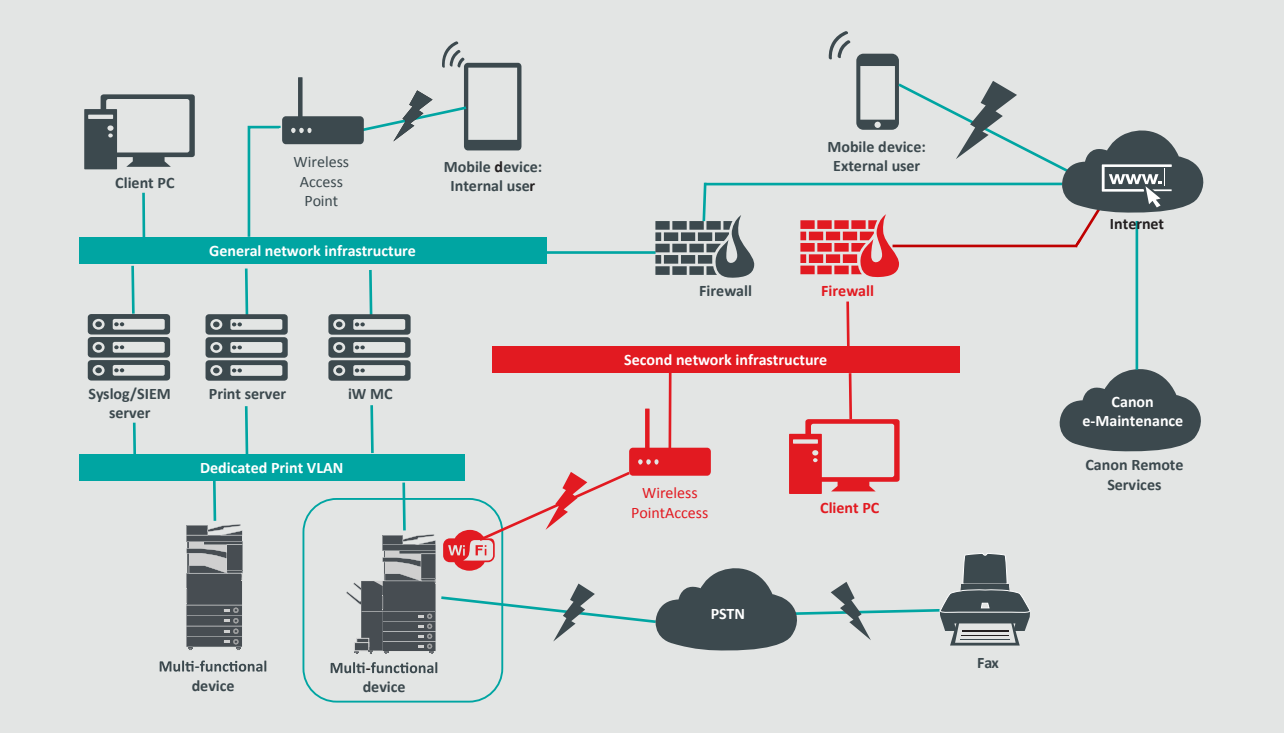
# EEN KANTOOROMGEVING IN EEN GROTE ONDERNEMING

Dit is meestal een multi-site, multi-kantoor omgeving met een gesegmenteerde netwerkarchitectuur. Hierbij worden meerdere MFD's ingezet op een afzonderlijk VLAN, toegankelijk voor intern gebruik via printserver(s). Deze MFD's zijn niet toegankelijk via het internet.

Deze omgeving heeft meestal een permanent team ter ondersteuning van netwerk- en back office-vereisten, evenals voor algemene computerproblemen, maar hierbij wordt verondersteld dat zij geen specifieke MFD-training hebben

Dit is meestal een multi-site, multi-kantoor omgeving met een gesegmenteerde netwerkarchitectuur. Hierbij worden meerdere MFD's ingezet op een afzonderlijk VLAN, toegankelijk voor intern gebruik via printserver(s). Deze MFD's zijn niet toegankelijk via het internet.

**Afbeelding 2** Kantoorwerk in een grote onderneming




Rood gemarkeerde verbindingen zijn beschikbaar vanaf modellen van generatie 3

# CONFIGURATIE-OVERWEGINGEN

Neem in acht dat, tenzij er hierna een functie van de imageRUNNER ADVANCE wordt vermeld, de standaardinstellingen voor dit bedrijf en deze netwerkomgeving als voldoende worden beschouwd.

**Tabel 2** Configuratie-overwegingen kantooromgeving in een grote onderneming

| Functie imageRUNNER ADVANCE | Beschrijving | Overweging |
|---|---|---|
| Servicemodus | Voor toegang tot instellingen Servicemodus | Wachtwoordbeveiliging met een niet-standaard, niet-triviaal wachtwoord met een maximumlengte |
| Servicemanagement-systeem | Hiermee hebt u toegang tot verschillende niet-standaard apparaatinstellingen | Wachtwoordbeveiliging met een niet-standaard, niet-triviaal wachtwoord met een maximumlengte |
| SMB bekijken/verzenden | Opslaan onder en opvragen vanuit Windows / SMB-netwerkshares | Systeembeheerders moeten, op basis van beleid, alle gebruikers verbieden lokale accounts op hun machine te creëren voor gebruik bij het het delen van documenten met de imageRUNNER ADVANCE via SMB |
| Externe gebruikersinterface | Web-based configuratietool | Na initiële apparaatconfiguraties de externe gebruikersinterface volledig uitschakelen door uitschakelen van HTTP en HTTPS |
| SNMP | Integratie netwerkcontrole | Versie 1 uitschakelen en versie 3 inschakelen |
| Naar e-mail en/of IFAX verzenden | E-mails met bijlagen vanaf apparaat verzenden | SSL inschakelen<br>Activeren:<br>- Certificaatverificatie bij de SMTP-server<br>Of, indien niet uitvoerbaar:<br>- Deze functie alleen gebruiken in een omgeving met een Network Intruder Detection System-collector Geen POP3-verificatie gebruiken voor verzenden SMTP SMTP-verificatie gebruiken |
| POP3 | Automatisch documenten vanuit mailbox opvragen en printen | SSL inschakelen<br>Activeren:<br>- Certificaatverificatie bij de POP3-server<br>Of, indien niet uitvoerbaar:<br>- Deze functie alleen gebruiken in een omgeving met een Network Intruder Detection System-collector POP3-verificatie inschakelen |
| Adresboek / LDAP | Directoryservice gebruiken voor het opzoeken van telefoonnummer of e-mailadressen voor verzending van scans | SSL inschakelen<br>Activeren:<br>- Certificaatverificatie bij de LDAP-server<br>Of, indien niet uitvoerbaar:<br>- Deze functie alleen gebruiken in een omgeving met een Network Intruder Detection System-collector Geen domeingegevens voor verificatie met de LDAP-server gebruiken; LDAP-specifieke gegevens gebruiken |
| IPP | Printopdrachten via IP verbinden en verzenden | IPP uitschakelen |
| WebDAV verzenden | Documenten op een externe locatie scannen en opslaan | Verificatie voor WebDAV-shares inschakelen SSL inschakelen<br>Afdwingen dat de printer alleen de upload van bestanden met “printbestandextensies” toestaat |
| IEEE802.1X | Mechanisme voor netwerktoegangsverificatie | EAPOL V1 ondersteund |
| Gecodeerde PDF | Documenten coderen | Op basis van beleid mogen vertrouwelijke documenten alleen gecodeerd worden met behulp van PDF versie 1.6 (AES-128) |
| Gecodeerde Secure Print | Beveiliging van Secure Print verbeteren door codering van het bestand en het wachtwoord tijdens overdracht | Gebruikersnaam op het tabblad Printer in de client-printerconfiguratie configureren naar een andere gebruikersnaam dan de LDAP-/domeingegevens van de betreffende gebruiker.<br>Controleren dat “Printopdrachten beperken” uitgeschakeld is |
| Certificate Auto Enrolment | Het automatische inschrijvingsproces verbetert de efficiëntie van het ophalen en implementeren van digitale certificaten | Vereist een netwerkcertificaatoplossing om te profiteren |
| Melding Syslog-gebeurtenis | Het System Logging Protocol is een standaardprotocol dat wordt gebruikt om systeemlog- of gebeurtenisberichten te verzenden naar een specifieke server die Syslog-server wordt genoemd | Overweeg de Syslog-gegevens van imageRUNNER ADVANCE te verwijzen naar uw bestaande Syslog-analysetool voor netwerken of naar het SIEM-platform (Security Event Management System) voor ondernemingen. |
| Verify-systeem bij het opstarten | Biedt de zekerheid dat de softwarecomponenten van het systeem niet in gevaar zijn gebracht. Dit heeft een minimale impact op de opstarttijd van het systeem | Functie activeren |
| Draadloze LAN | Biedt wireless toegang | WPA-PSK/WPA2-PSK met sterke wachtwoorden gebruiken |
| WiFi Direct | Gebruikt voor het tot stand brengen van een WiFi Direct-verbinding | WiFi Direct uitschakelen |
| Embedded webbrowser (beschikbaar vanaf 2e versie modellen van generatie 3) | Browsertoegang tot internet | Gepaste beperkingen toepassen of mogelijkheid tot download van via de browser verkregen bestanden uitschakelen |

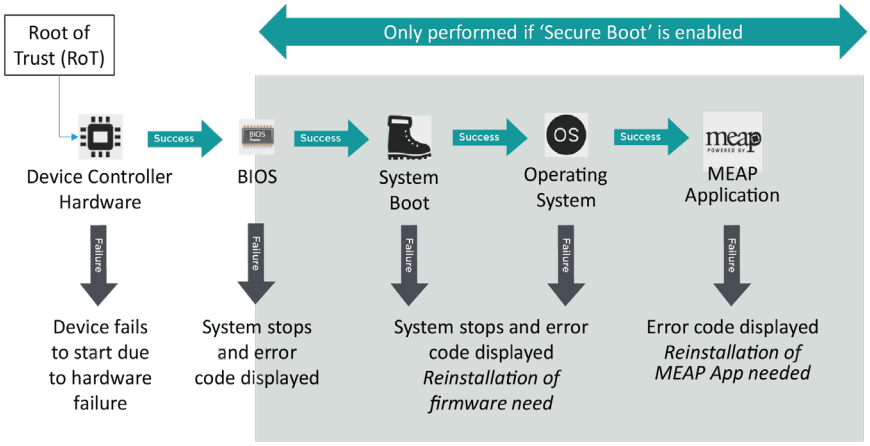
De nieuwste generatie van imageRUNNER ADVANCE-modellen bieden draadloze netwerkconnectiviteit, waardoor het apparaat met een WiFi-netwerk verbonden kan worden en tegelijkertijd met een bedraad netwerk verbonden is. Dit scenario kan nuttig zijn wanneer de klant moet een apparaat moet delen tussen twee netwerken. Een schoolomgeving is een typisch voorbeeld waarin aparte personeel- en leerlingnetwerken worden gebruikt.

Het imageRUNNER ADVANCE-platform biedt een functieomgeving voor flexibel gebruik. Met de protocollen en services die beschikbaar zijn om dit te bereiken, is het belangrijk om ervoor te zorgen dat alleen de vereiste functies, services en protocollen zijn ingeschakeld om aan de behoeften van de gebruiker te voldoen. Dit is een goede veiligheidspraktijk en zal de potentiële aanvalsoppervlakte verminderen en hun exploitatie verhinderen. Aangezien er voortdurend nieuwe kwetsbaarheden verschijnen, moet er altijd op worden gelet dat het apparaat niet wordt aangetast, zowel intrinsiek als extrinsiek. De mogelijkheid om gebruikersactiviteiten te controleren is nuttig om te helpen bij het identificeren en nemen van corrigerende maatregelen wanneer dat nodig is.

ImageRUNNER ADVANCE-softwareplatform versie 3.8 biedt enkele extra functies voor degenen die al een aantal jaren beschikbaar zijn. Deze omvatten de mogelijkheid om het apparaat in real-time te controleren met behulp van Syslog en Verify System bij het opstarten. Het gebruik van deze functies in samenwerking met uw bestaande netwerkbeveiligingsoplossingen, zoals een Security Information Event Management-platform of een logboekoplossing, biedt een breder inzicht in en de identificatie van incidenten en voor forensische doeleinden.

## Verify-systeem bij het opstarten

Deze functionaliteit is een hardwaremechanisme dat is ontworpen om ervoor te zorgen dat alle onderdelen van de imageRUNNER ADVANCE Generation 3 III Edition-systeemsoftware worden gecontroleerd aan de hand van een vertrouwensbasis om ervoor te zorgen dat het besturingssysteem wordt geladen zoals Canon dat beoogt. Als een kwaadwillende partij het systeem probeert te wijzigen of als er een fout optreedt bij het laden van het systeem, wordt het proces gestopt en wordt er een foutcode weergegeven.



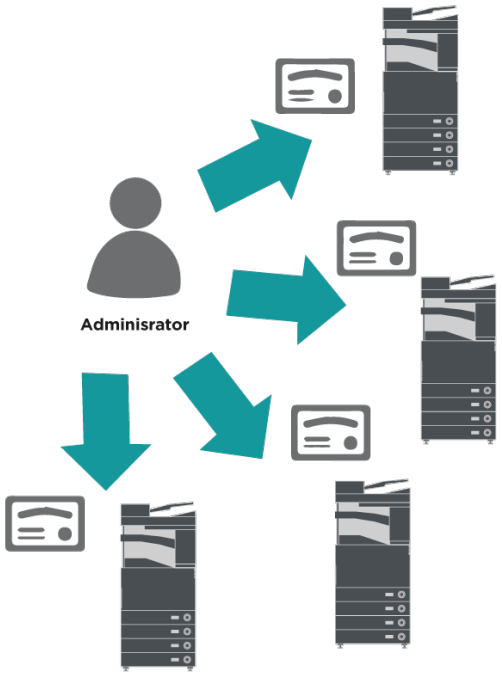

**Afbeelding 3** Proces van Verify-systeem bij het opstarten

Dit proces is transparant voor de gebruiker, naast dat op het display wordt aangegeven dat er een oneigenlijke systeemversie wordt geladen. De imageRUNNER ADVANCE Generation 3 III Edition heeft een optie om Verify-systeem bij opstarten in te schakelen. Deze optie moet worden ingeschakeld om deze beveiligingsfunctie in te schakelen.

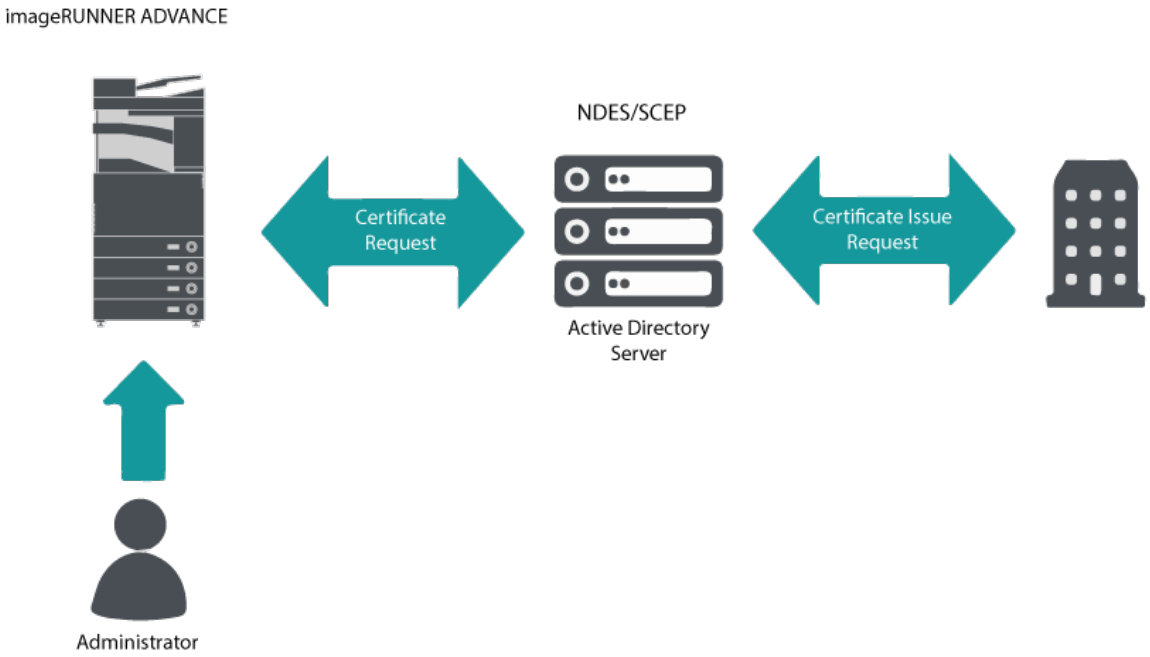
## Certificate Auto Enrolment

In versies van het imageRUNNER ADVANCE-systeemsoftwareplatform ouder dan versie 3.8 moest de beheerder handmatig bijgewerkte beveiligingscertificaten op elk apparaat installeren. Dit is een arbeidsintensieve taak omdat er om de beurt verbinding met elk apparaat moet worden gemaakt om een handmatige update uit te voeren. Certificaten moeten handmatig worden geïnstalleerd met behulp van de externe gebruikersinterface (RUI) van het specifieke apparaat, waardoor het proces veel meer tijd kost. Met de service Certificate Auto Enrolment die is geïntroduceerd vanaf platformversie 3.8 en hoger, is deze overhead geëlimineerd.

Het automatische inschrijvingsproces verbetert de efficiëntie bij het ophalen van certificaten. Het biedt de mogelijkheid om automatisch certificaten op te halen met behulp van de Network Device Enrollment Service (NDES) voor Microsoft Windows en het Simple Certificate Enrollment Protocol (SCEP).




**Afbeelding 4** Inschrijving van certificaten




**Afbeelding 5** Inschrijvingsproces voor certificaten

SCEP is een protocol dat certificaten ondersteunt die zijn uitgegeven door een certificeringsinstantie (CA) en met NDES kunnen netwerkapparaten certificaten ophalen of bijwerken op basis van SCEP.

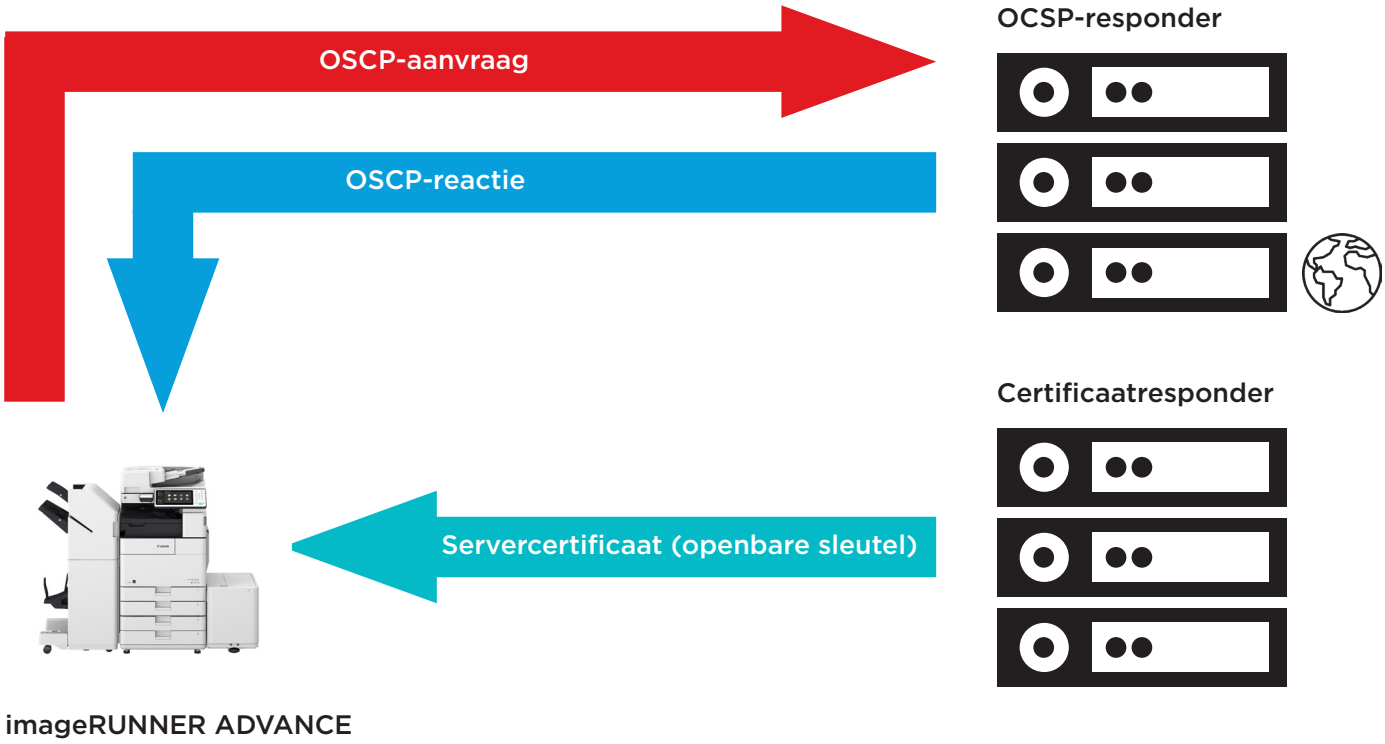
NDES is een rolservice van de Active Directory Certificate Services.

## Online statusprotocol voor certificaten

Er zijn een aantal redenen waarom het nodig kan zijn om een digitaal certificaat in te trekken. Voorbeelden hiervan zijn onder andere het verlies van de persoonlijke sleutel, het verlies van de sleutel, het verlies van de sleutel of het wijzigen van een domeinnaam.

Het Online Certificate Status Protocol (OCSP) is een standaard Internet-protocol dat wordt gebruikt voor het controleren van de intrekkingsstatus van een digitaal X.509-certificaat dat is geleverd door de Certificate Server. Door een OCSP-aanvraag te verzenden naar de OCSP-responder (meestal een uitgever van een certificaat) en een specifiek certificaat op te geven, antwoordt de OCSP-responder met een 'goed', 'verzonden' of 'onbekend'.

**Afbeelding 6** OCSP-proces voor het schudden van handen




Met imageRUNNER ADVANCE van Platform versie 3.10 biedt OCSP een real-time mechanisme om de geïnstalleerde X.509 digitale certificaten te controleren. Eerdere platformversies ondersteunde alleen CRL-methode (Certificate Revoke List), die inefficiënt is en leidt tot zware overhead op netwerkbronnen.

## Beveiligingsinformatie en gebeurtenisbeheer

De imageRUNNER ADVANCE-technologie ondersteunt de mogelijkheid om real-time beveiligingsgebeurtenissen uit te voeren met behulp van het Syslog-protocol dat voldoet aan RFC 5424, RFC 5425 en RFC 5426.

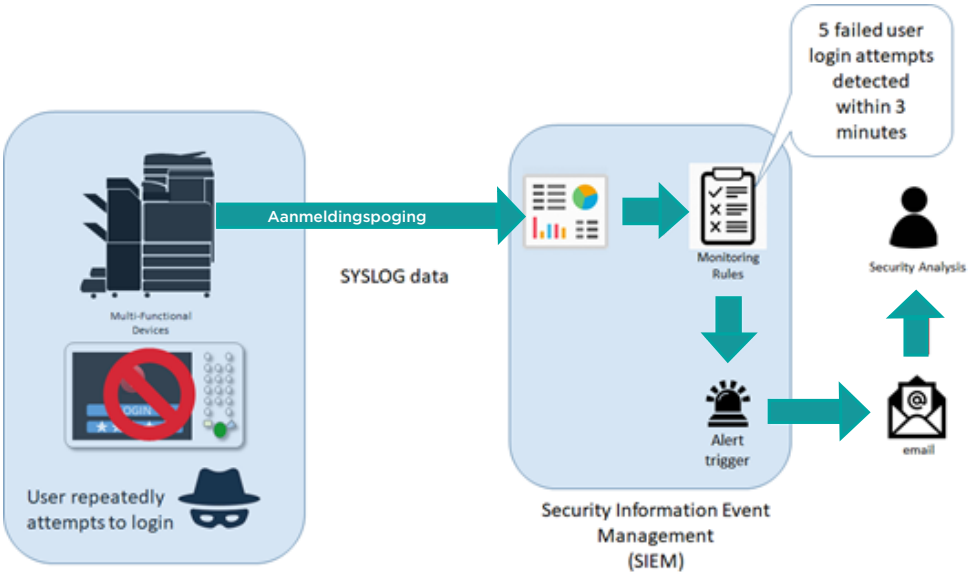
Dit protocol wordt door een groot aantal apparaattypen gebruikt om real-time informatie te verzamelen die kan worden gebruikt om potentiële beveiligingsproblemen te identificeren.

Om het detecteren van bedreigingen en beveiligingsincidenten te vergemakkelijken, moet het apparaat zo worden geconfigureerd dat het verwijst naar een SIEM-server (Security Incident Event Management) van derden.

Syslog-gebeurtenissen die door het apparaat worden gegenereerd, kunnen worden gebruikt om acties te maken door middel van het in real-time verzamelen en analyseren van gebeurtenissen uit een groot aantal contextuele gegevensbronnen (Afbeelding 7). De oplossing kan ook compliancerapportage en incidentonderzoek ondersteunen door het gebruik van aanvullende oplossingen, zoals een SIEM-server. Een voorbeeld is te zien in afbeelding 8.

De nieuwste generatie imageRUNNER ADVANCE-apparaten biedt Syslog-functionaliteit die een reeks gebeurtenissen ondersteunt die kunnen worden verzameld. Dit kan worden gebruikt om gebeurtenissen in een aantal ongelijksoortige bronnen te correleren en te analyseren om trends of afwijkingen te identificeren.


**Afbeelding 7** Vastleggen Syslog-gegevens




**Afbeelding 8** Voorbeeld van gebruik van Syslog-gegevens imageRUNNER ADVANCE

## Beheer van logbestanden op het apparaat

Naast de Syslog-functionaliteit van systeemsoftwareplatform versie 3.8, heeft de imageRUNNER ADVANCE de volgende logboeken die op het apparaat kunnen worden beheerd. Deze logboeken kunnen worden geëxporteerd in CSV-bestandsindeling via de externe gebruikersinterface (RUI).

**Tabel 3** - Voorbeelden van logbestanden die kunnen worden beheerd door het multifunctionele apparaat.

| Logtype | Nummer aangegeven als 'Logtype' in het CSV-bestand | Beschrijving |
|---|---|---|
| Log | 4098 | Dit logboek bevat informatie met betrekking tot de verificatiestatus van gebruikersverificatie (aanmelden/afmelden en geslaagde/mislukte gebruikersverificatie), het registreren/wijzigen/verwijderen van gebruikersgegevens die worden beheerd met gebruikersverificatie, en het beheer (toevoegen/bewerken/verwijderen) van rollen met het ACCESS MANAGEMENT SYSTEM |
| Taaklogboek | 1001 | Dit logboek bevat informatie over het voltooien van kopieer-, fax-, scan-, verzend- en printtaken |
| Transmissielogboek | 8193 | Dit logboek bevat informatie met betrekking tot transmissies |
| Logboek voor Advanced Space-opslag | 8196 | Dit logboek bevat informatie over het opslaan van bestanden in Advanced Space, Network (Advances Space van andere apparaten) en Memory Media |
| Bewerkingslogboek van de mailbox | 8197 | Dit logboek bevat informatie over de bewerkingen die worden uitgevoerd op gegevens in de mailbox, het Postvak IN voor Memory RX en het Postvak IN voor vertrouwelijke faxen |
| Verificatielogboek voor mailboxen | 8199 | Dit logboek bevat informatie met betrekking tot de verificatiestatus van de mailbox, het Postvak IN voor Memory RX en het Postvak IN voor vertrouwelijke faxen |
| Logboek voor geavanceerde ruimtebewerkingen | 8201 | Dit logboek bevat informatie over gegevensbewerkingen in de Advanced Space |
| Logboek apparaatbeheer | 8198 | Dit logboek bevat informatie over het starten/uitschakelen van het apparaat, wijzigingen die zijn aangebracht in de instellingen met behulp van de functie Settings/Registration, wijzigingen die zijn aangebracht in de instellingen met behulp van de functie Device Information Delivery, en de tijdinstelling. Het logboek voor apparaatbeheer registreert ook wijzigingen in gebruikersinformatie of beveiligingsinstellingen wanneer het apparaat wordt geïnspecteerd of gerepareerd door uw plaatselijke erkende Canon-dealer |
| Netwerkverificatielogboek | 8200 | Dit logboek wordt vastgelegd wanneer IPSec-communicatie mislukt |
| Logboek Alles exporteren/importeren | 8202 | Dit logboek bevat informatie over het importeren/exporteren van de instellingen met de functie Export All/Import All |
| Back-uplogboek van mailbox | 8203 | Dit logboek bevat informatie over het maken van back-ups van gegevens in de mailbox van gebruikers, het Postvak IN voor Memory RX, het Postvak IN voor vertrouwelijke faxen, de Advanced Space, eventuele gegevens in de wachtrij en het formulier dat is geregistreerd voor de functie Superimpose Images |
| Logboek voor bewerkingen op het scherm toepassings-/softwarebeheer | 3101 | Dit is een bewerkingslogboek voor SMS (Service Management Service), softwareregistratie/-updates en installatieprogramma's van MEAP-toepassingen, enzovoort |
| Logboek beveiligingsbeleid | 8204 | Dit logboek bevat informatie over de status van de instellingen van het beveiligingsbeleid |
| Logboek groepsbeheer | 8205 | Dit logboek bevat informatie over de status van de instellingen (registreren/bewerken/verwijderen) van de gebruikersgroepen |
| Logboek systeemonderhoud | 8206 | Dit logboek bevat informatie met betrekking tot firmware-updates en het maken van back-ups/herstellen van de MEAP-toepassing, enzovoort |
| Logboek verificatieprint | 8207 | Dit logboek bevat informatie en de geschiedenis van de bewerkingen met betrekking tot printtaken met geforceerde wachtstand |
| Logboek instellingsynchronisatie | 8208 | Dit logboek bevat informatie over de synchronisatie van apparaatinstellingen. Instellingen synchroniseren voor meerdere multifunctionele printers van Canon |
| Logboek voor controlelogdatabeheer | 3001 | Dit logboek bevat informatie met betrekking tot het starten en beëindigen van deze functie (de functie Audit Log Management), evenals het exporteren van logboeken, enzovoort |

Logboeken kunnen maximaal 40.000 records bevatten. Zodra het aantal records meer dan 40.000 bedraagt, worden de oudste records eerst verwijderd.

# ONDERSTEUNING VOOR EXTERNE APPARATEN

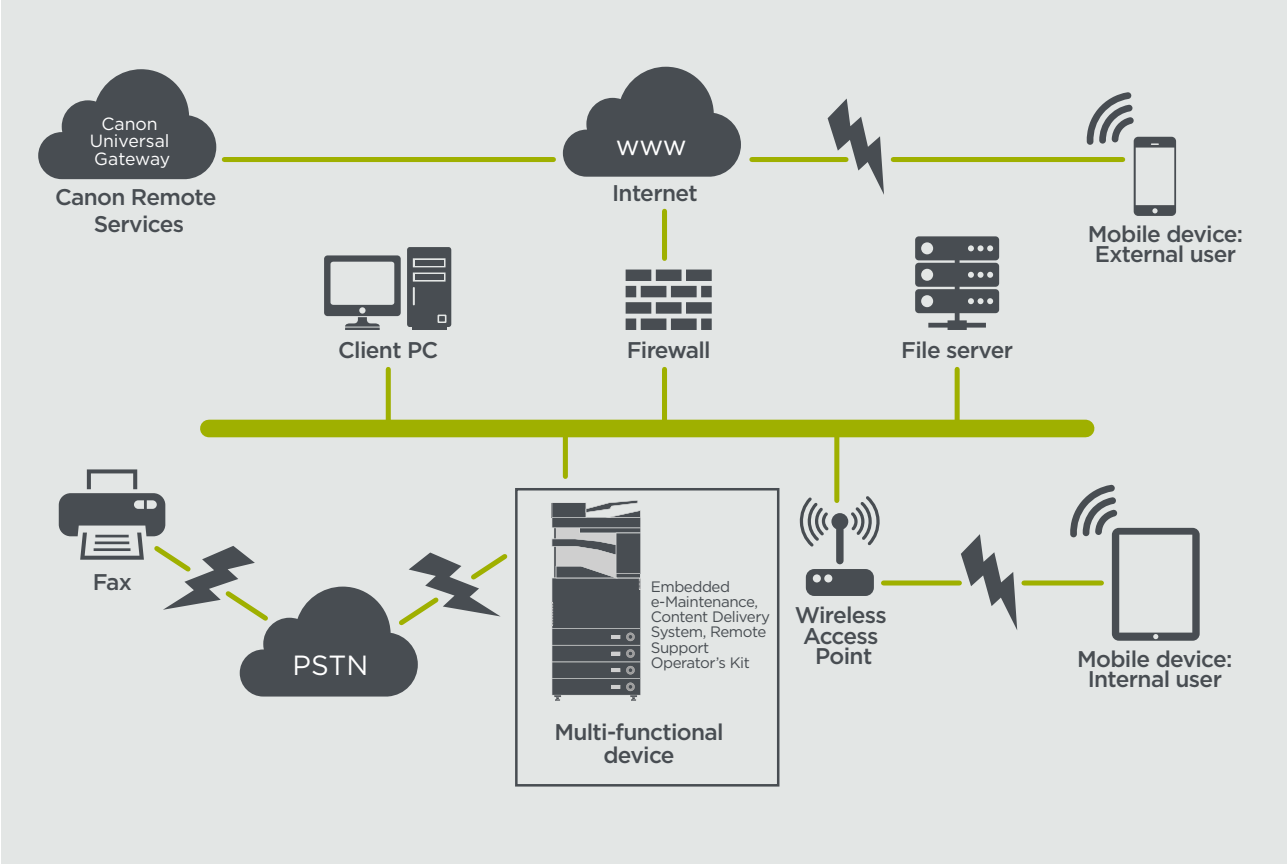
Voor een efficiënte dienstverlening door Canon of een Canon-partner kan de imageRUNNER ADVANCE servicegerelateerde gegevens verzenden, alsmede firmware-updates van softwareapplicaties ontvangen. Neem in acht dat er geen afbeeldingen of metagegevens van afbeeldingen worden verzonden.

Hieronder worden twee mogelijke implementaties van externe diensten van Canon binnen een bedrijfsnetwerk getoond.

## Implementatiescenario 1: Verspreide verbinding

Bij deze instelling staat elke MFD een directe verbinding met de externe dienst via het internet toe.

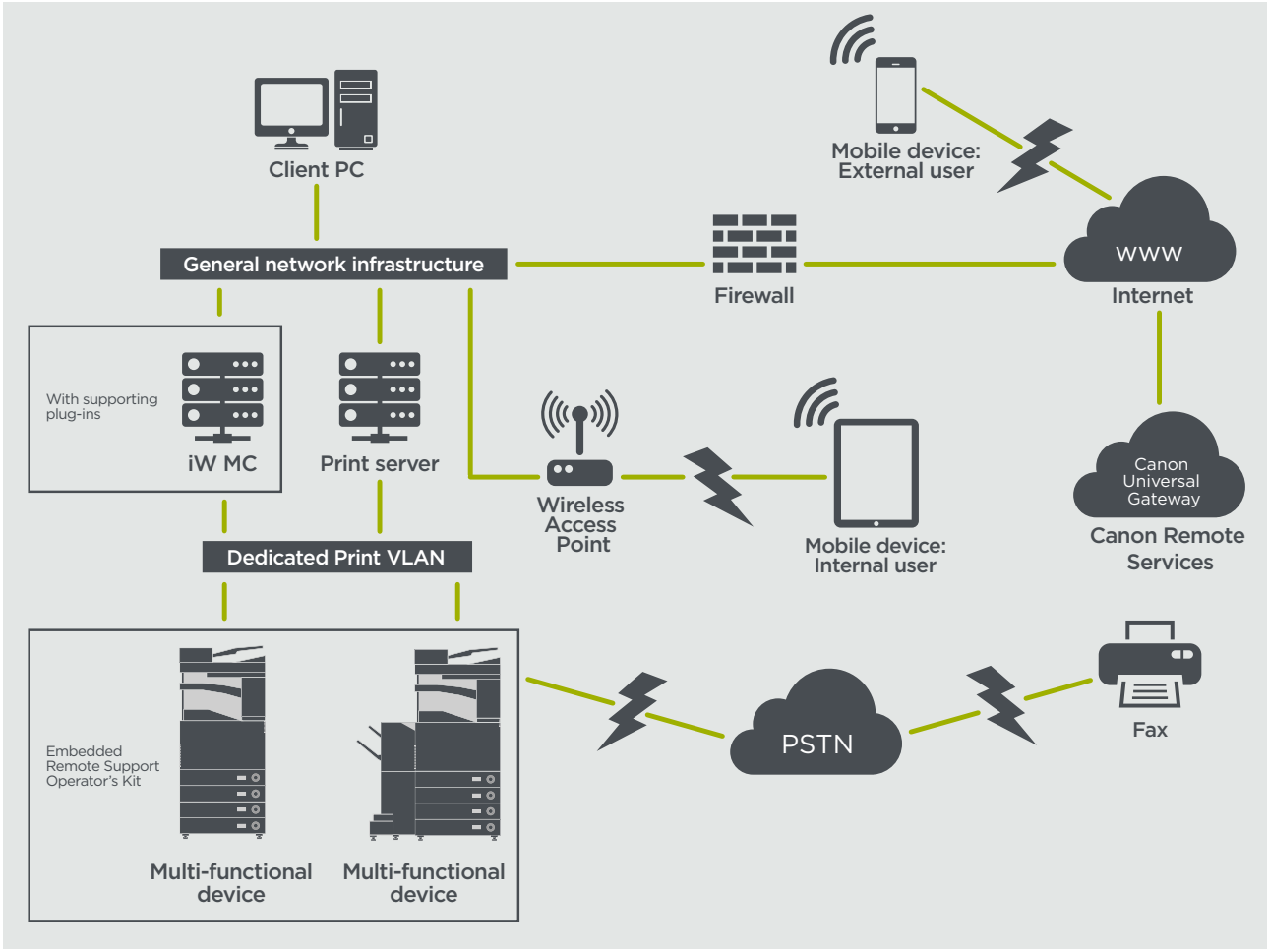
**Afbeelding 9** Verspreide verbinding



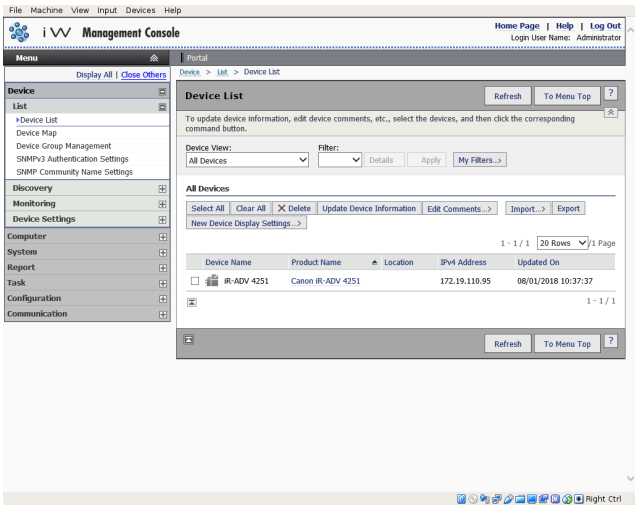

## Implementatiescenario 2: Gecentraliseerd beheerde verbinding

In een omgevingsscenario voor een grote onderneming, waarbij meerdere MFD's worden ingezet, bestaat de behoefte om deze apparaten efficiënt vanuit één centraal punt te kunnen beheren, en dit omvat de verbinding met externe diensten van Canon. Om de holistische beheeraanpak te vergemakkelijken, zouden afzonderlijke apparaten beheerverbindingen tot stand brengen via een enkel iW Management Console (iWMC)-verbindingspunt. Voor communicatie tussen de Device Firmware Upgrade (DFU) plug-in en multifunctionele apparaten, wordt UDP-poort 47545 gebruikt.

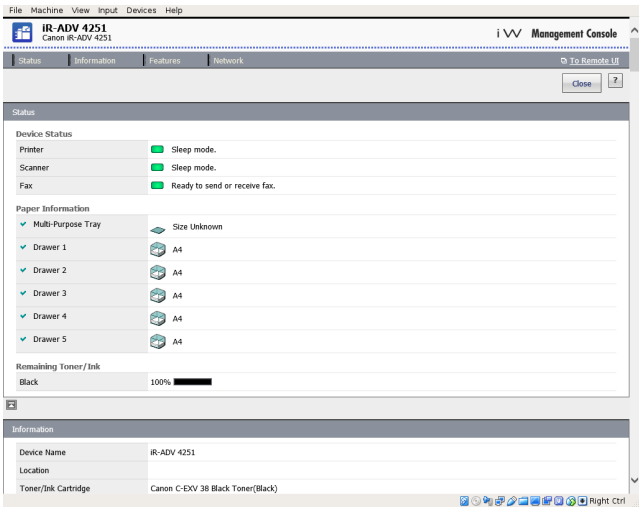
**Afbeelding 10** Centraal beheerde verbinding




**Afbeelding**
**11a.** Apparatenlijst (in dit geval één enkel apparaat) zoals aangeduid op imageWARE Management Console en
**11b.** Apparaatgegevens en instellingen




**Afbeelding 11a**




**Afbeelding 11b**

## e-Maintenance

Het e-Maintenance-systeem biedt een geautomatiseerde manier van het verzamelen van apparaatgebruiktellers voor factureringsdoeleinden, verbruiksartikelenbeheer en externe apparaatcontrole door middel van status- en storingswaarschuwingen.

Het e-Maintenance-systeem bestaat uit een internetgerichte server (UGW) en embedded software voor multifuntionele apparaten (eRDS) en/of aanvullende server-based software (RDS plug-in) voor het verzamelen van servicegerelateerde informatie voor het apparaat. De eRDS is een controleprogramma dat in de imageRUNNER ADVANCE wordt uitgevoerd. Als de controle-optie in de instellingen van het apparaat ingeschakeld is, verkrijgt de eRDS zijn eigen apparaatinformatie en verzendt deze naar de UGW. De RDS plug-in is een controleprogramma dat op een algemene PC wordt geïnstalleerd en 1 tot 3.000 apparaten kan controleren. Het programma verkrijgt de informatie van elk apparaat via het netwerk en verzendt deze naar de UGW.

Zoals afgebeeld in de onderstaande tabel 4 wordt op de volgende pagina een overzicht gegeven van de gegevensoverdracht, de protocollen (afhankelijk van de geselecteerde opties tijdens ontwerp en implementatie) en de gebruikte poorten. Op geen enkel moment worden afbeeldingsgegevens van kopieën, prints, scans of faxen overgedragen.

**Tabel 4** Gegevensoverzicht e-Maintenance

| Beschrijving | Verwerkte gegevens | Protocol/poort | Poort |
|---|---|---|---|
| Communicatie tussen eMaintenance (eRDS of RDS plug-in) en UGW | UGW webservice-adres<br>Proxy-serveradres / poortnummer<br>Proxy-account / wachtwoord<br>UGW-mail-doeladres<br>SMTP-serveradres<br>POP-serveradres<br>Informatie apparaatstatus, teller en model<br>Serienummer<br>Informatie resterende toner/inkt<br>Informatie firmware<br>Informatie over reparatieaanvraag<br>Registratie-informatie<br>Serviceoproep<br>Service-alarm<br>Storing<br>Milieu<br>Conditielogboek | HTTP/HTTPS/SMTP/POP3 | TCP/80 TCP/443 TCP/25 TCP/110 |
| Communicatie tussen eMaintenance en apparaat (alleen RDS plug-in, want eRDS is embedded software) | | SNMP<br>Van Canon<br>SLP/SLP/HTTPS | UDP/161 TCP/47546,<br>UDP/47545, TCP9007 UDP/427<br>UDP/11427 TCP/443 |

## Content Delivery System

Het Content Delivery System (CDS) brengt een verbinding tussen het MFD en de Canon Universal Gateway (UGW) tot stand. Het biedt apparaatfirmware en applicatie-updates.

**Tabel 5** Gegevensoverzicht Content Delivery System

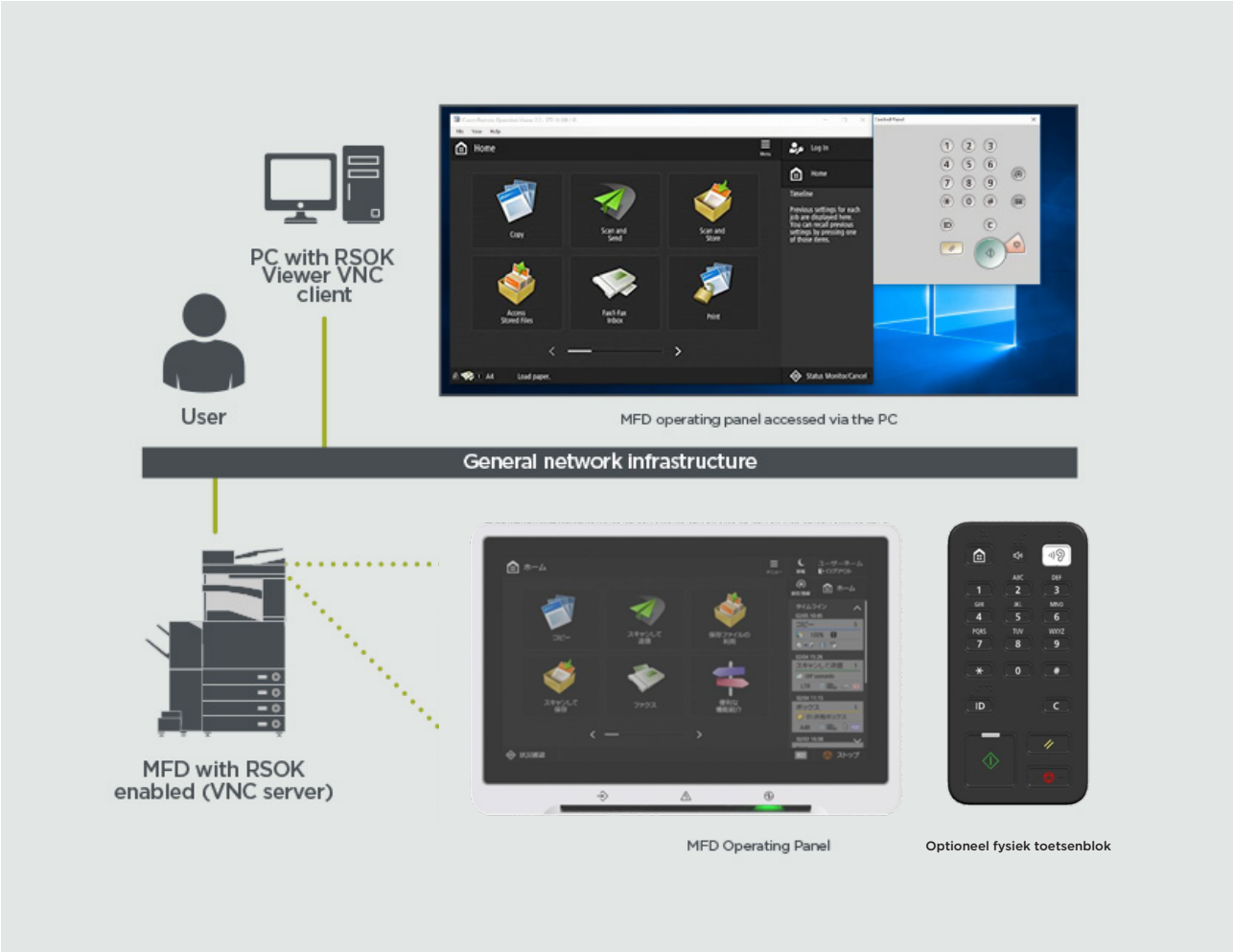
| Beschrijving | Verzonden gegevens | Protocol/poort | Poort |
|---|---|---|---|
| Communicatie tussen MFD en UGW | Serienummer van apparaat<br>Firmwareversie<br>Taal<br>Land<br>Informatie met betrekking tot EULA apparaat | HTTP/HTTPS | TCP/80<br>TCP/443 |
| Communicatie tussen UGW en MFD | Testbestand (willekeurige binaire gegevens) voor communicatietest<br><br>Binaire gegevens firmware of MEAP-applicatie | HTTP/HTTPS | TCP/80<br>TCP/443 |

Een specifieke URL voor CDS-toegang is vooraf in de apparaatconfiguratie ingesteld. Als centraal beheer van apparaat-firmware en applicaties vanuit de infrastructuur nodig is, dan is een lokale installatie van iWMC met de Device Firmware Upgrade (DFU) plug-in en de Device Application Management plug-in vereist.

## Remote Support Operator's Kit

De Remote Support Operator's Kit (RSOK) biedt externe toegang tot het bedieningspaneel van het apparaat. Dit server-client systeemtype bestaat uit een VNC-server die draait op de MFP- en Remote Operation Viewer VNC Microsoft Windows client-applicatie.

**Afbeelding 12** Setup Remote Support Operator's Kit (RSOK)




**Tabel 6** Gegevensoverzicht Remote Support Operator's Kit

| Beschrijving | Verzonden gegevens | Protocol/poort | Poort |
|---|---|---|---|
| VNC-wachtwoordverificatie | Gebruikerswachtwoord | DES-codering | 5900 |
| Operation Viewer | Bedieningspaneel apparaat<br>- schermgegevens<br>- bediening hardware-sleutel | Versie 3.3 RFB-protocol | 5900 |

# BIJLAGE

## Beveiligingsgerelateerde functies Canon imageRUNNER ADVANCE

Het imageRUNNER ADVANCE-platform biedt externe configuratie via een webservice-interface die bekend staat als de externe gebruikersinterface (RUI, Remote User Interface). Deze interface biedt toegang tot veel van de configuratie-instellingen van het apparaat en kan indien niet toegestaan worden uitgeschakeld en kan met een wachtwoord beveiligd worden om onbevoegde toegang te voorkomen.

Terwijl de meeste apparaatinstellingen beschikbaar zijn via de RUI, moet het bedieningspaneel van het apparaat gebruikt worden om items in te stellen die niet met behulp van deze interface kunnen worden ingesteld. Wij raden u aan ongebruikte services uit te schakelen en de controles op de benodigde services aan te scherpen. Voor flexibiliteit en ondersteuning biedt de Remote Support Operator's Kit (RSOK) externe toegang tot het bedieningspaneel van het apparaat. Deze is gebaseerd op VNC-technologie bestaande uit een server (de MFD) en een client (een netwerk-PC). Er is een specifieke Canon client-PC viewer beschikbaar, die waar nodig gesimuleerde toegang tot de toetsen van het bedieningspaneel biedt.

In dit gedeelte wordt een overzicht gegeven van de belangrijkste beveiligingsgerelateerde functies van de imageRUNNER ADVANCE en de bijbehorende configuratie-instellingen.

Interactieve online gebruikershandleidingen zijn beschikbaar op https://oip.manual.canon/ en geven niet alleen informatie over beveiligingsfuncties. Selecteer eerst het juiste producttype (bijvoorbeeld imageRUNNER ADVANCE DX), klik op het zoekpictogram en voer uw zoekcriteria in. Hieronder zijn een paar algemene gebieden die het overwegen waard zijn.

### Machinebeheer

Om het lekken van persoonlijke informatie of onbevoegd gebruik te verhinderen, zijn constante en efficiënte beveiligingsmaatregelen vereist. Door het aanwijzen van een beheerder voor het controleren van de apparaatinstellingen, kunnen het gebruikersbeheer en de beveiligingsinstellingen tot uitsluitend bevoegden worden beperkt.

Wijs de onderstaande koppeling aan in uw webbrowser en voer de **configuratie van de beheerder** in het zoekvak in. Dit geeft informatie met betrekking tot:

- Basisbeheer van het apparaat
- Beperking van risico's door nalatigheid, gebruikersfouten en misbruik
- Apparaatbeheer
- Beheer van systeemconfiguratie en instellingen

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

### IEEE P2600-norm

Een aantal imageRUNNER ADVANCE-modellen voldoen aan de IEEE P2600-norm, een wereldwijde informatiebeveiligingsnorm voor multifunctionele randapparatuur en printers.

Via de onderstaande link vindt u een beschrijving van de beveiligingsvereisten die in de IEEE 2600-norm gedefinieerd worden en van de manier waarop de apparaatfuncties aan deze vereisten voldoen.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

### IEEE 802.1X-verificatie

Wanneer een verbinding met een 802.1 X-netwerk nodig is, moet het apparaat verifiëren dat het een toegestane verbinding betreft.

Wijs uw webbrowser aan op de onderstaande koppeling en voer **802.1X** in het zoekvak in.
https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Beveiligingsbeleid op machine toepassen**

Met de nieuwste imageRUNNER ADVANCE-modellen zijn beveiligingsinstellingen voor meerdere apparaten mogelijk, waarbij het beveiligingsbeleid in batchvorm kan worden beheerd via de RUI. Er kan een afzonderlijk wachtwoord worden gebruikt, waarmee alleen de beveiligingsbeheerder de instellingen kan wijzigen.

Wijs uw webbrowser aan op de onderstaande koppeling en voer **een beveiligingsbeleid toepassen op de computer** in het zoekvak in.  Dit geeft informatie met betrekking tot:

- Wachtwoordgebruik ter bescherming van beveilingsbeleidinstellingen
- Configureren van de beveilingsbeleidinstellingen
- Items voor beveilingsbeleidinstellingen

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Gebruikersbeheer**

Klanten die een hoger niveau van beveiliging en efficiëntie vereisen, kunnen gebruikmaken van de ingebouwde functionaliteit of een printbeheeroplossing zoals uniFLOW.

Neem voor meer informatie over Canon-printbeheeroplossingen contact op met lokale vertegenwoordigers van Canon of raadpleeg de uniFLOW-productbrochure.

**Configureren van de beveilingsbeleidinstellingen**

Bevoegde gebruikers kunnen onverwachte verliezen oplopen als gevolg van schadelijke aanvallen door derden, zoals sniffing, spoofing en de manipulatie van gegevens tijdens overdracht in een netwerk. Om uw belangrijke en waardevolle informatie te tegen deze aanvallen te beschermen, ondersteunt de machine vele functies ter verbetering van de beveiliging en privacy.

Wijs de onderstaande koppeling naar uw webbrowser en typ **Netwerkbeveiligingsinstellingen configureren** in het zoekvak.  Dit geeft informatie met betrekking tot:

Via de onderstaande link vindt u informatie over:

- Onbevoegde toegang voorkomen
- Verbinding maken met een draadloos LAN
- Inrichten van de netwerkomgeving

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

**Beheer van harde schijf-gegevens**

De harde schijf van het apparaat wordt gebruikt voor de opslag van het besturingssysteem, de configuratie-instellingen en de opdrachtinformatie van het apparaat. De meeste apparaatmodellen bieden volledige encryptie van de schijf (conform FIPS 140-2), waardoor deze gekoppeld is aan het betreffende apparaat en niet door onbevoegde gebruikers gelezen kan worden. Een voorbereidende Canon MFP Security Chip is gecertificeerd als een cryptografische module onder het Cryptographic Module Validation Program (CMVP) dat is opgericht door Amerika en Canada, evenals volgens het Japanse Cryptographic Module Validation Program (JCMVP).

Wijs uw webbrowser aan op de onderstaande koppeling en voer **gegevens op de harde schijf beheren** in het zoekvak in.

https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

# OVERZICHT VAN BEVEILIGINGSBELEIDINSTELLINGEN

Bij de derde generatie van de imageRUNNER ADVANCE-modellen zijn de beveiligingsbeleidinstellingen en beveiligingsbeheergebruiker geïntroduceerd. Hierbij is succesvol inloggen door de beheerder vereist en, indien geconfigureerd, een aanvullende login van de beveiligingsbeheerder met een extra wachtwoord.

In de onderstaande tabel worden de beschikbare instellingen beschreven.

| 1. Interface | Opmerkingen |
|---|---|
| **Beleid wireless verbinding** | |
| Gebruik van Direct-verbinding niet toestaan | <Use Wi-Fi Direct> is ingesteld op <Off><br>Toegang tot de het apparaat vanaf mobiele apparaten is niet mogelijk |
| Gebruik van wireless LAN verbieden | <Select Wired/Wireless LAN> is ingesteld op <Wired LAN><br>Het tot stand brengen van een wireless verbinding met het apparaat via een wireless LAN-router of -toegangspunt is niet mogelijk |
| **Beleid USB** | |
| Gebruik als USB-apparaat niet toestaan | <Use as USB Device> is ingesteld op <Off><br>U kunt de print- of scanfuncties vanaf via USB aangesloten PC's niet gebruiken wanneer het gebruik als USB-apparaat niet toegestaan is |
| Gebruik als USB-opslagapparaat niet toestaan | <Use USB Storage Device> is ingesteld op <Off><br>Het gebruik van USB-opslagapparaten is niet mogelijk<br>De volgende servicefuncties werken echter wel als Prohibit use as USB storage device is ingesteld op ON<br>• Firmware-update via USB-stick (vanuit download-modus)<br>• Subloggegevens van apparaat naar USB kopiëren (LOG2USB)<br>• Rapport van apparaat naar USB kopiëren (RPT2USB) |
| **Bedrijfsbeleid netwerkcommunicatie**<br>Opmerking: deze instellingen zijn niet van toepassing op communicatie met IEEE 802.1 X-netwerken, zelfs als het selectievakje is aangevinkt voor [Always Verify Server Certificate When Using TLS] | |
| Altijd handtekeningen voor SMS/ WebDAV-serverfuncties verifiëren | In <SMB Server Settings> zijn de opties <Require SMB Signature for Connection> en <Use SMB Authentication> ingesteld op <On>, en <Use TLS> in <WebDAV Server Settings> is ingesteld op <On><br>Wanneer het apparaat wordt gebruikt als een SMB-server of WebDAV-server worden de digitale certificaathandtekeningen tijdens de communicatie geverifieerd |
| Altijd servercertificaat verifiëren bij gebruik TLS | <Confirm TLS Certificate for WebDAV TX>, <Confirm TLS Certificate for SMTP TX>, <Confirm TLS Certificate for POP RX>, <Confirm TLS Certificate for Network Access> en <Confirm TLS Certificate Using MEAP Application> zijn allemaal ingesteld op <On>, en er is een vinkje aanwezig bij <CN><br><br>Bovendien zijn de opties <Verify Server Certificate> en <Verify CN> in <SIP Settings> > <TLS Settings> ingesteld op <On><br><br>Tijdens TLS-communicatie wordt verificatie uitgevoerd voor digitale certificaten en hun gemeenschappelijke namen |
| Verificatie leesbare tekst voor serverfuncties niet toestaan | • <Use FTP Printing> in <FTP Print Settings> is ingesteld op <Off><br>• <Allow TLS (SMTP RX)> in <E-Mail/I-Fax Settings> <Communication Settings> is ingesteld op <Always TLS>, <Dedicated Port Authentication Method> in <Network> is ingesteld op <Mode 2>,<br>• <Use TLS> in <WebDAV Server Settings> is ingesteld op <On><br>Wanneer de machine als een server wordt gebruikt, zijn geen functies beschikbaar die van verificatie van normale tekst gebruik maken<br>TLS wordt gebruikt als verificatie van leesbare tekst niet is toegestaan. Bovendien kunt u geen gebruikmaken van applicaties of serverfuncties, zoals FTP, die alleen verificatie van leesbare tekst ondersteunen<br>Toegang tot de machine vanaf apparaatbeheersoftware of -driver is wellicht niet mogelijk |
| Gebruik van SNMPv1 niet toestaan | In <SNMP Settings> is <Use SNMPv1> ingesteld op <Off><br>U kunt de apparaatinformatie in de printerdriver of beheersoftware mogelijk niet opvragen of instellen, als het gebruik van SNMPv1 niet toegestaan is |
| **Beleid poortgebruik** | |
| LPD-poort beperken | Poortnummer: 515<br><LPD Print Settings> is ingesteld op <Off><br>Het uitvoeren van LPD-printen is niet mogelijk |
| RAW-poort beperken | Poortnummer 9100<br><RAW Print Settings> is ingesteld op <Off><br>RAW-printen is niet mogelijk |
| FTP-poort beperken | Poortnummer 21<br>In <FTP Print Settings> is <Use FTP Printing> ingesteld op <Off><br>FTP-printen is niet mogelijk |
| WSD-poort beperken | Poortnummer 3702, 60000<br>In <WSD Settings> zijn de opties <Use WSD>, <Use WSD Browsing> en <Use WSD Scan> allemaal ingesteld op <Off><br>Het gebruik van WSD-functies is niet mogelijk |
| BMLinkS-poort beperken | Poortnummer 1900<br>Niet gebruikt in Europese regio |
| IPP-poort beperken | Poortnummer 631<br>U kunt geen gebruik maken van Mopria, AirPrint en IPP als de IPP-poort beperkt is |

| | |
|---|---|
| SMB-poort beperken | Poortnummer: 137, 138, 139, 445<br>In <SMB Server Settings> is <Use SMB Server> ingesteld op <Off><br>Het gebruik van het apparaat als een SMB-server is niet mogelijk |
| SMTP-poort beperken | Poortnummer 25<br>In <E-Mail/I-Fax Settings> > <Communication Settings> is <SMTP RX> ingesteld op <Off><br>SMTP-ontvangst is niet mogelijk |
| Specifieke poort beperken | Poortnummer: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547<br>U kunt geen gebruik maken van de functies remote copy, remote fax, remote scan of remote print, of applicaties, enz. als de specifieke poort beperkt is |
| Poort Remote Operator's Software beperken | Poortnummer 5900<br><Remote Operation Settings> is ingesteld op <Off><br>Het gebruik van bedieningsfuncties op afstand is niet mogelijk |
| SIP (IP Fax)-poort beperken | Poortnummer: 5004, 5005, 5060, 5061, 49152<br><Use Intranet> in <Intranet Settings>, <Use NGN> in <NGN Settings> en <Use VoIP Gateway> in <VoIP Gateway Settings> zijn allemaal ingesteld op <Off><br>Het gebruik van IP fax is niet mogelijk |
| mDNS-poort beperken | Poortnummer 5353<br>In <mDNS Settings> zijn de opties <Use IPv4 mDNS> en <Use IPv6 mDNS> ingesteld op <Off><br><Use Mopria> is ingesteld op <Off><br>Het is niet mogelijk om in het netwerk te zoeken of automatische instellingen uit te voeren met mDNS. Het is ook niet mogelijk om te printen met Mopria™ of AirPrint |
| SLP-poort beperken | Poortnummer 427<br>In <Multicast Discovery Settings> is <Response> ingesteld op <Off><br>Zoeken in het netwerk of het uitvoeren van automatische instellingen met behulp van SLP is niet mogelijk |
| SNMP-poort beperken | Poortnummer 161<br>U kunt de apparaatinformatie in de printerdriver of beheersoftware mogelijk niet opvragen of instellen, als de SNMP-poort beperkt is<br>In <SNMP Settings> zijn de opties <Use SNMPv1> en <Use SNMPv3> ingesteld op <Off> |

| 2. Verificatie | Opmerkingen |
|---|---|
| **Bedrijfsbeleid verificatie** | |
| Gastgebruikers niet toestaan | • <Advanced Space Settings> > <Authentication Management> is ingesteld op <On><br>• <Login Screen Display Settings> is ingesteld op <Display When Device Operation Starts><br>• <Restrict Job from Remote Device without User Auth> is ingesteld op <On><br>Niet-geregistreerde gebruikers kunnen zich niet aanmelden bij het apparaat. Printopdrachten die vanaf een computer zijn verzonden, worden ook geannuleerd |
| Instelling van automatisch uitloggen afdwingen | Deze instelling is voor het afmelden via het bedieningspaneel. Dit geldt niet voor andere methoden voor het afmelden (instelbaar bereik 10 sec - 9 minuten)<br><Auto Reset Time> is ingeschakeld. De gebruiker wordt automatisch afgemeld als er gedurende een bepaalde periode geen bewerkingen worden uitgevoerd<br>Selecteer [Time Until Logout] op het Remote UI-instelscherm |
| **Bedrijfsbeleid wachtwoord** | |
| Caching van wachtwoord voor externe servers niet toestaan | Deze instelling geldt niet voor wachtwoorden die de gebruiker expliciet opslaat, zoals wachtwoorden voor adresboeken, enz.<br><Prohibit Caching of Authentication Password> is ingesteld op <On><br>Gebruikers moeten altijd een wachtwoord invoeren voor toegang tot een externe server |
| Waarschuwing weergeven wanneer standaard wachtwoord in gebruik is | <Display Warning When Default Password Is in Use> is ingesteld op <On><br>Er wordt een waarschuwingsbericht weergegeven wanneer het standaard fabriekswachtwoord van het apparaat wordt gebruikt |
| Gebruik van standaard wachtwoord voor externe toegang niet toestaan | <Allow Use of Default Password for Remote Access> is ingesteld op <Off><br>Het is niet mogelijk het standaard fabriekswachtwoord te gebruiken voor toegang tot de machine vanaf een computer |
| **Beleid wachtwoordinstellingen (het beleid geldt niet voor afdelings-ID-beheer of PIN)** | |
| Minimumaantal tekens voor wachtwoord instellen | Minimumaantal tekens instelbaar tussen 1 en 32 |
| Geldigheidsperiode wachtwoord instellen | Geldigheidsperiode instelbaar tussen 1 en 180 dagen |
| Gebruik van 3 of meer identieke opeenvolgende tekens niet toestaan | |
| Gebruik van minstens 1 hoofdletter afdwingen | |
| Gebruik van minstens 1 kleine letter afdwingen | |
| Gebruik van minstens 1 cijfer afdwingen | |
| Gebruik van minstens 1 symbool afdwingen | |
| **Beleid voor vergrendeling** | |
| Vergrendeling inschakelen | Geldt niet voor afdelings-ID/mailbox-PIN, PIN of Secure Print-verificatie, enz.<br>Vergrendelingsdrempel: instelbaar van 1 - 10 keer<br>Vergrendelingsperiode: instelbaar van 1 - 60 minuten |
| **3. Sleutel/certificaat** | **Opmerkingen** |
| Gebruik van zwakke encryptie niet toestaan | Geldt voor IPSec, TLS, Kerberos, S/MIME, SNMPv3 en wireless LAN<br>U mag niet kunnen communiceren met apparaten die uitsluitend zwakke encryptie ondersteunen |

| | |
|---|---|
| Gebruik van sleutel/certificaat met zwakke encryptie niet toestaan | Geldt voor IPSec, TLS en S/MIME<br>Als u een sleutel/certificaat met zwakke encryptie voor TLS gebruikt, wordt deze gewijzigd in de sleutel/het certificaat die/dat vooraf geïnstalleerd werd. U kunt niet communiceren als u een sleutel/certificaat met zwakke encryptie voor andere functies dan TLS gebruikt |
| TPM voor opslaan van wachtwoord en sleutel gebruiken | Alleen beschikbaar voor apparaten met TPM geïnstalleerd. Maak altijd een back-up van de TPM-sleutels als TPM is ingeschakeld. Raadpleeg de gebruikershandleiding voor meer informatie<br><br>Belangrijk wanneer TPM-instellingen ingeschakeld zijn:<br>• Zorg dat de standaardwaarde van het beheerderwachtwoord veranderd wordt, om te voorkomen dat derden een back-up van de TPM-sleutel kunnen maken. Als derden de TPM-back-up sleutel pakken, kunt u de TPM-sleutel niet herstellen.<br>• Voor een verbeterde beveiliging kan er slechts eenmaal een back-up van de TPM-sleutel worden gemaakt. Zorg dat u, als de TPM-instellingen ingeschakeld zijn, een back-up van de TPM-sleutel op een USB-geheugenapparaat maakt en deze op een veilige plek bewaart om verlies of diefstal te voorkomen<br>• De beveilingsfuncties van TPM garanderen geen volledige bescherming van gegevens en hardware. |

| 4. Log | Opmerkingen |
|---|---|
| Opslaan van controlelog afdwingen | • <Save Operation Log> ingesteld op <On><br>• <Display Job Log> is ingesteld op <On><br>• <Retrieve Job Log with Management Software> in <Display Job Log> is ingeteld op <Allow><br>• <Save Audit Log> is ingesteld op <On><br>• <Retrieve Network Authentication Log> is ingesteld op <On><br>Controlelogs worden altijd opgeslagen wanneer deze instelling ingeschakeld is |
| SNTP-instellingen afdwingen | SNTP-serveradres invoeren<br>In <SNTP Settings> is <Use SNTP> ingesteld op <On> Tijdsynchronisatie via SNTP is vereist. Voer een waarde in voor [Server Name] op het Remote UI-instelscherm |
| Rapportage syslog-logboek | Schakel Syslog-bestemmingsgegevens in bij gebruik van een Syslog-server of SIEM<br>• <gebruikersnaam en wachtwoord><br>• <SMB-servernaam><br>• <doelpad><br>• <exporttijd uitvoeren> |

| 5. Taak | Opmerkingen |
|---|---|
| **Printbeleid** | |
| Direct printen van ontvangen opdrachten niet toestaan | Ontvangen opdrachten worden opgeslagen in het fax/I-Fax-geheugen als direct printen van ontvangen opdrachten niet is toegestaan<br>• <Handle Files with Forwarding Errors> is ingesteld op <Off><br>• <Use Fax Memory Lock> is ingesteld op <On><br>• <Use I-Fax Memory Lock> is ingesteld op <On><br>• <Memory Lock End Time> is ingesteld op <Off><br>• <Display Print When Storing from Printer Driver> in <Set/Register Confidential Fax Inboxes> is ingesteld op <Off><br>• <Settings for All Mail Boxes> > <Print When Storing from Printer Driver> is ingesteld op <Off><br>• <Box Security Settings> > <Display Print When Storing from Printer Driver> is ingesteld op <Off><br>• <taak van onbekende gebruiker verbieden> is ingesteld op <aan> en <geforceerd vasthouden> is ingesteld op <aan> het afdrukken vindt niet onmiddellijk plaats, zelfs niet wanneer er afdrukbewerkingen worden uitgevoerd |
| **Beleid verzenden/ontvangen** | |
| Alleen verzenden naar geregistreerde adressen toestaan | In <Limit New Destination> zijn de opties <Fax>, <E-Mail>, <I-Fax> en <File> ingesteld op <On><br>Verzenden is alleen mogelijk naar bestemmingen die in het adresboek geregistreerd zijn |
| Bevestiging van faxnummer afdwingen | Gebruikers moeten het faxnummer bij het verzenden van een fax ter bevestiging opnieuw invoeren |
| Automatisch doorsturen niet toestaan | <Use Forwarding Settings> is ingesteld op <Off><br>Automatisch faxen doorsturen is niet mogelijk. |

| 6. Opslag | Opmerkingen |
|---|---|
| Volledig wissen van gegevens afdwingen | <Hard Disk Data Complete Deletion> is ingesteld op <On> |

Raadpleeg de productwebsite op https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/ voor de volledige imageRUNNER ADVANCE-specificaties.

**Canon Belgium NV/SA**
Berkenlaan 3
1831 Diegem
Tel. 02-722 04 11
Fax 02-721 32 74
canon.be

**Canon Nederland N.V.**
Brabantlaan 2
5216 TV 's-Hertogenbosch
Telefoon: (073) 6 815 815
Fax: (073) 6 120 685
canon.nl

**Canon Inc.**
Canon.com

**Canon Nederland**
canon.nl

Dutch edition v1.0