HARDENING GUIDE TIL MFP'ER

imageRUNNER ADVANCE

Canon

INTRODUKTION

Moderne Canon-multifunktionsprintere (MFP'er) leverer print-, kopierings-, scannings-, afsendelses- og faxfunktioner. MFP'er er selvstændige computerservere, der leverer en række netværkstjenester og kan lagre store mængder data på deres harddiske.

Når en virksomhed implementerer disse printere i deres infrastruktur, er der en række områder, der skal behandles som en del af den overordnede sikkerhedsstrategi, som skal beskytte fortroligheden, integriteten og tilgængeligheden af jeres netværkssystemer.

Implementeringer vil uden tvivl være forskellige fra virksomhed til virksomhed, og hver virksomhed vil have sine egne, specifikke sikkerhedskrav. Mens vi arbejder sammen om at sikre, at Canon-løsninger leveres med behørige sikkerhedsindstillinger, bestræber vi os på yderligere at understøtte dette ved at levere en række konfigurationsindstillinger, så I bedre kan tilpasse enheden til maskinen i jeres specifikke situation.

Dette dokument er udarbejdet med henblik på at give jer tilstrækkelige oplysninger til, at I kan drøfte de bedst egnede indstillinger for jeres miljø med Canon eller Canon-partneren. Det skal bemærkes, at ikke al hardware på enheden har samme funktionsniveau, og at forskellig systemsoftware kan give forskellig funktionalitet. Når der er truffet en beslutning om den endelige konfiguration, kan den anvendes på jeres enhed eller flåde. Du er velkommen til at kontakte Canon eller en Canon-partner for at få yderligere oplysninger og support.

Hvem er dette dokument beregnet til?

Dette dokument henvender sig til alle, der beskæftiger sig med design, implementering og sikring af multifunktionsprintere på kontorer i en netværksinfrastruktur. Dette kan omfatte IT- og netværksspecialister, IT-sikkerhedseksperter og servicepersonale.

Omfang og dækning

Vejledningen forklarer og rådgiver om konfigurationsindstillingerne for to typiske netværksmiljøer, så virksomheder kan implementere en løsning for MFP'er på en sikker måde og ud fra bedste praksis. Den forklarer også (fra systemsoftwareplatform version 3.8), hvordan Syslog-funktionen kan give feedback i realtid fra MFP'en. Disse indstillinger er blevet testet og godkendt af Canons sikkerhedsteam.

Vi tager ikke hensyn til specifikke lovkrav i en bestemt branche, som kan stille andre sikkerhedskrav, og disse er ikke medtaget i dette dokument.

Denne vejledning er udviklet på baggrund af det typiske funktionssæt for imageRUNNER ADVANCE-platformen, og selvom oplysningerne heri gælder for alle modeller og serier i imageRUNNER ADVANCE-porteføljen, kan visse funktioner variere fra model til model.

Implementering af passende sikkerhed for MFP'er i jeres miljø

For at undersøge de sikkerhedsmæssige konsekvenser af at implementere en MFP som en del af jeres netværk har vi taget to typiske scenarier i betragtning:

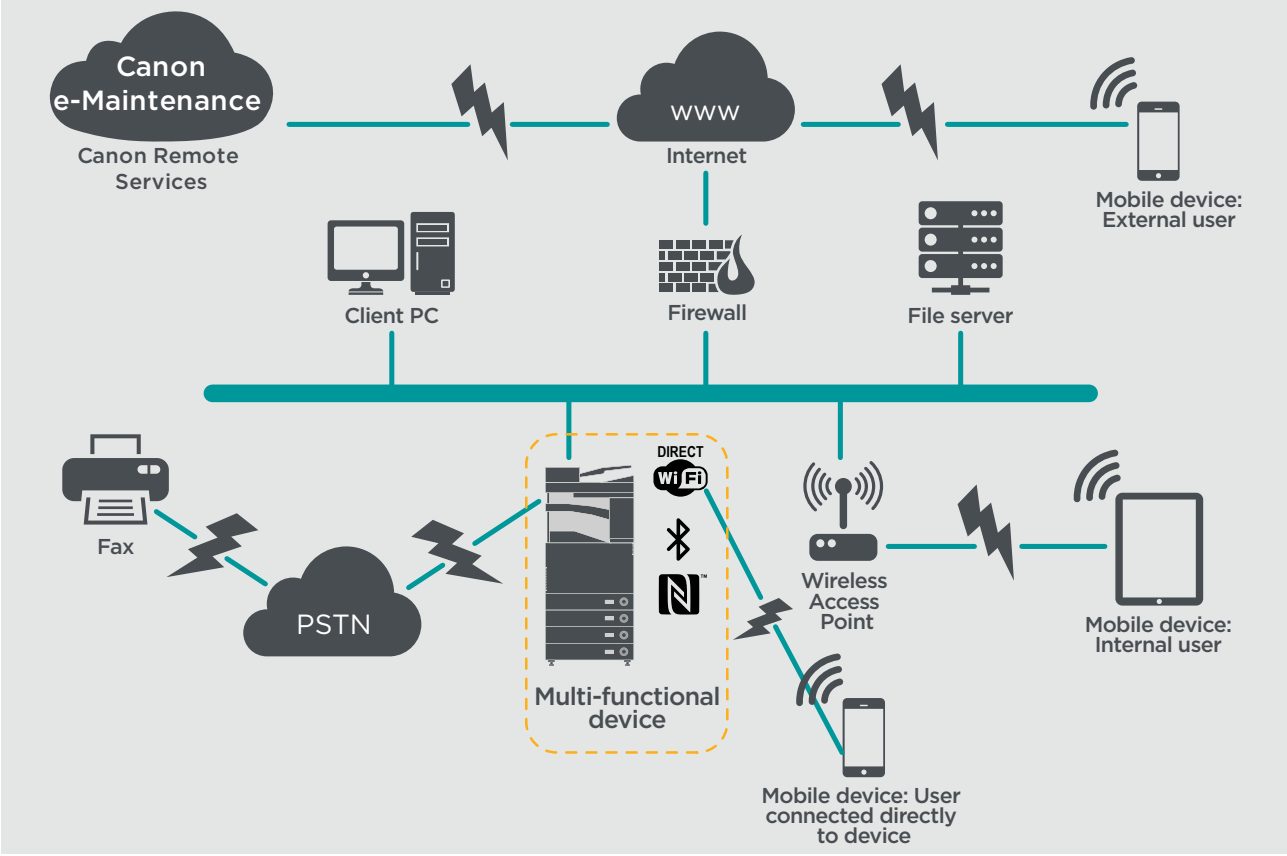
- **Et typisk mindre kontormiljø**
- **Et større virksomhedskontormiljø**

MINDRE KONTORMILJØ

Dette vil typisk være et mindre virksomhedsmiljø med en ikke-segmenteret netværkstopologi. Det bruger en eller to multifunktionsprintere til intern brug, og disse printere er ikke tilgængelige på internettet.

Selvom mobilt print er tilgængeligt, er yderligere løsningskomponenter påkrævet. For brugere, der har brug for printertjenester uden for et LAN-miljø, kræves der en sikker forbindelse, men dette er ikke dækket af denne vejledning. Der skal dog tages hensyn til sikkerheden for de data, der sendes mellem fjernenheden og printinfrastrukturen.

Figur 1 Mindre kontornetværk



Den nyeste generation af imageRUNNER ADVANCE-modeller har trådløs netværksforbindelse, så de kan oprette forbindelse til et Wi-Fi-netværk. De kan også bruges til at oprette en punkt-til-punkt Wi-Fi Direct-forbindelse til en mobil enhed uden behov for en netværksforbindelse.

Bluetooth- og NFC-funktionerne er tilgængelige for flere enhedsmodeller og bruges kun til at oprette Wi-Fi Direct-forbindelse til iOS- og Android-enheder.

KONFIGURATIONSKRAV

Bemærk, at medmindre en funktion i imageRUNNER ADVANCE er nævnt nedenfor, anses den for at være tilstrækkelig i standardindstillingerne for dette virksomheds- og netværksmiljø.

Tabel 1 Konfigurationskrav i et mindre kontormiljø

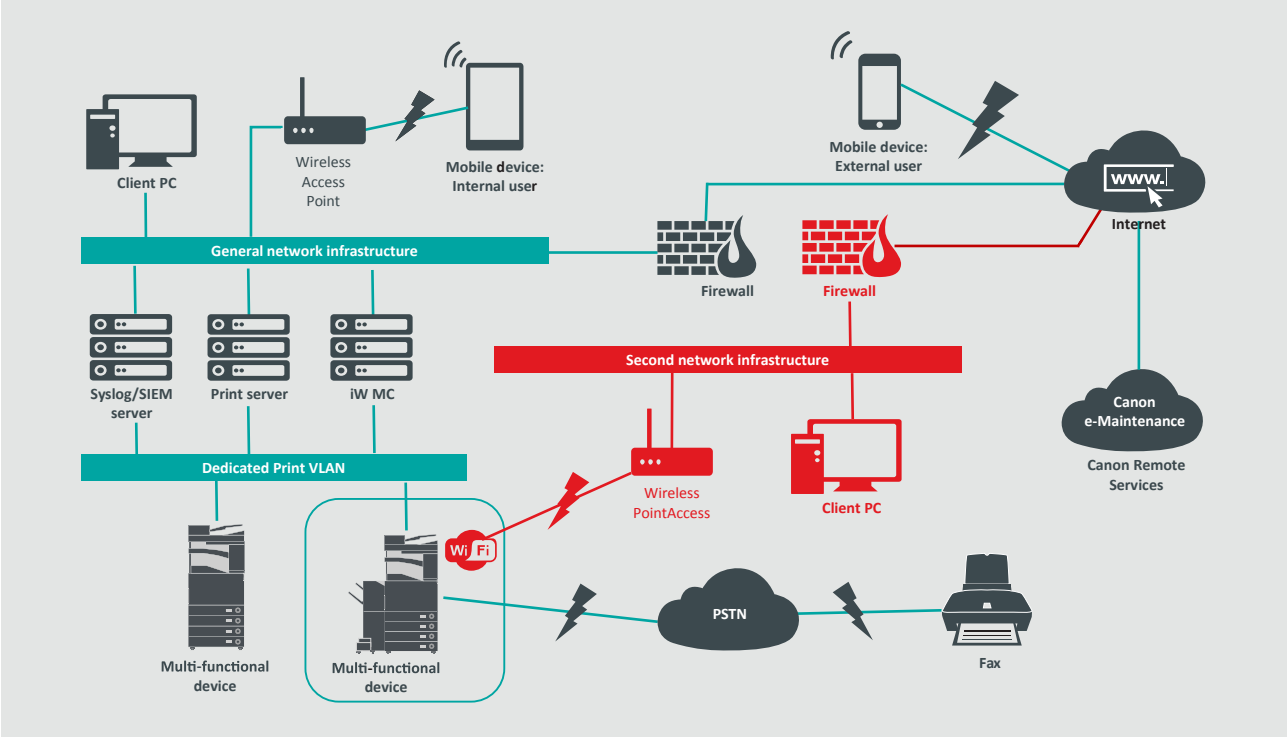
imageRUNNER ADVANCE-funktion	Beskrivelse	Krav
Servicefunktion	Giver adgang til indstillinger for servicefunktionen	Beskyt med adgangskode med en ikke-standardiseret og ikke-triviel adgangskode med maksimal længde
Serviceadministrationssystem	Giver adgang til forskellige ikke-standardiserede enhedsindstillinger	Beskyt med adgangskode med en ikke-standardiseret og ikke-triviel adgangskode med maksimal længde
Gennemse/send SMB	Gem og hent til og fra Windows/SMB-netværksdelinger	Systemadministratorer bør – ifølge politikken – nægte brugere tilladelse til at oprette lokale konti på deres klientmaskine til brug ved deling af dokumenter med imageRUNNER ADVANCE via SMB
Fjernbrugerinterface	Webbaseret konfigurationsværktøj	imageRUNNER ADVANCE-administratoren skal aktivere HTTPS for fjernbrugerinterfacet og deaktivere HTTP-adgang. Aktivér brugen af en PIN-godkendelse, der er unik for hver enhed
SNMP	Integration af netværksovervågning	Deaktivér version 1, og aktivér kun version 3
Send til e-mail og/eller IFAX	Send e-mails fra MFP'en med vedhæftede filer	Aktivér SSL Brug ikke POP3-godkendelsen før SMTP-afsendelse Brug SMTP-godkendelse
POP3	Hent og print automatisk dokumenter fra mailboksen	Aktivér SSL Aktivér POP3-godkendelse
Adressebog/LDAP	Brug bibliotekstjenesten til at søge efter hjemmenumre eller e-mailadresser, som scanninger skal sendes til	Aktivér SSL Brug ikke domænelegitimationsoplysninger til at godkende over for LDAP-serveren. Brug LDAP-specifikke legitimationsoplysninger
FTP-print	Upload og download dokumenter til og fra den integrerede FTP-server	Aktivér FTP-godkendelse. Vær opmærksom på, at FTP-trafik altid vil overføres i klar tekst over netværket
WebDAV-afsendelse	Scan og gem dokumenter på en ekstern placering	Aktivér godkendelse for WebDAV-delinger
Krypteret PDF	Kryptér dokumenter	Ifølge politikken bør følsomme dokumenter kun krypteres ved hjælp af PDF-version 1.6 (AES-128)
Sikkert print	Printjobbet sendes til enheden, men låses i printkøen, indtil den tilsvarende pinkode indtastes	Aktivér PIN-beskyttede printjob
Syslog-hændelsesnotifikation	Systemlogprotokollen er en standardindustriprotokol, der bruges til at sende systemlog- eller hændelsesmeddelelser til en bestemt server, der kaldes en Syslog-server	Overvej at henvise imageRUNNER Syslog-dataene til jeres eksisterende netværks systemloganalyseværktøj eller SIEM-platform (Enterprise Security Event Management System).
Bekræft system ved opstart	Giver sikkerhed for, at systemets softwarekomponenter ikke er blevet kompromitteret. Det vil have en minimal indvirkning på systemets opstartstid	Aktivér funktionen
Integreret webbrowser	Browseradgang til internettet	Gennemtving gennem administration brugen af en webproxy med indholdsfiltrering for at undgå, at der er adgang til skadeligt eller inficeret indhold. Deaktivér oprettelsen af favoritter
Bluetooth og NFC (tilgængeligt fra Generation 3-modeller)	Bruges til at oprette en Wi-Fi Direct-forbindelse	Aktivér Wi-Fi Direct for at tillade direkte forbindelse til en mobil enhed. Wi-Fi Direct kan ikke bruges, når Wi-Fi bruges til at oprette forbindelse til et netværk
Trådløst LAN	Giver trådløs adgang	Brug WPA-PSK/WPA2-PSK med stærke adgangskoder
IPP	Forbind og send printjob via IP	Deaktivér IPP

ET KONTORMILJØ I EN STOR VIRKSOMHED

Dette er typisk et miljø med flere lokaliteter og flere kontorer med en segmenteret netværksarkitektur. Det har flere multifunktionsprintere kørende på et separat VLAN, der er tilgængeligt til intern brug via printserver(e). Disse MFP'er er ikke tilgængelige fra internettet.

Dette miljø vil normalt have et fast team, der yder support til dets netværks- og backoffice-krav, og som hjælper med at afhjælpe computerproblemer, men her går vi ud fra, at dette team ikke har specifik uddannelse i MFP'er.

Figur 2 Kontorarbejde i den store virksomhed



Forbindelser, der er fremhævet med rødt, vil være tilgængelige fra Generation 3-modeller

KONFIGURATIONSKRAV

Bemærk, at medmindre en funktion i imageRUNNER ADVANCE er nævnt nedenfor, anses den for at være tilstrækkelig i standardindstillingerne for dette virksomheds- og netværksmiljø.

Tabel 2 Konfigurationskrav i større virksomhedskontormiljøer

imageRUNNER ADVANCE-funktion	Beskrivelse	Krav
Servicefunktion	Giver adgang til indstillinger for servicefunktionen	Beskyt med adgangskode med en ikke-standardiseret og ikke-triviel adgangskode med maksimal længde
Serviceadministrationssystem	Giver adgang til forskellige ikke-standard enhedsindstillinger	Beskyt med adgangskode med en ikke-standardiseret og ikke-triviel adgangskode med maksimal længde
Gennemse/send SMB	Gem og hent til og fra Windows/SMB-netværksdelinger	Systemadministratorer bør – ifølge sikkerhedspolitikken – nægte brugere tilladelse til at oprette lokale konti på deres maskine til brug ved deling af dokumenter med imageRUNNER ADVANCE via SMB
Fjernbrugerinterface	Webbaseret konfigurationsværktøj	Efter de indledende enhedskonfigurationer deaktiveres det eksterne fjernbrugerinterface fuldstændigt ved at deaktivere HTTP og HTTPS
SNMP	Integration af netværksovervågning	Deaktivér version 1, og aktivér kun version 3
Send til e-mail og/eller IFAX	Send e-mails fra MFP'en med vedhæftede filer	Aktivér SSL Aktivér: - Certifikatbekræftelse på SMTP-serveren Eller hvis det ikke er muligt: - Brug kun denne funktion i et miljø, hvor der findes et system til registrering af netværksindtrængen. Brug ikke POP3-godkendelsen før SMTP-afsendelse. Brug SMTP-godkendelse
POP3	Hent og print automatisk dokumenter fra mailboksen	Aktivér SSL Aktivér: - Certifikatbekræftelse på POP3-serveren Eller hvis det ikke er muligt: - Brug kun denne funktion i et miljø, hvor der findes et system til registrering af netværksindtrængen. Aktivér POP3-godkendelse
Adressebog/LDAP	Brug bibliotekstjenesten til at søge efter telefonnumre eller e-mailadresser, som scanninger skal sendes til	Aktivér SSL Aktivér: - Certifikatbekræftelse på LDAP-serveren Eller hvis det ikke er muligt: - Brug kun denne funktion i et miljø, hvor der et system til registrering af netværksindtrængen. Brug ikke domænelegitimationsoplysninger til at godkende over for LDAP-serveren. Brug LDAP-specifikke legitimationsoplysninger
IPP	Forbind og send printjob via IP	Deaktivér IPP
WebDAV-afsendelse	Scan og gem dokumenter på en ekstern placering	Aktivér godkendelse for WebDAV-delinger, Aktivér SSL, Gennemtving, at printeren kun tillader upload af filer, der ender med "filtypenavne til print", fx .doc eller .pdf
IEEE802.1X	Godkendelsesmekanisme for netværksadgang	EAPOL V1 understøttes
Krypteret PDF	Kryptér dokumenter	Følsomme dokumenter bør – ifølge sikkerhedspolitikken – kun krypteres ved hjælp af PDF-version 1.6 (AES-128)
Krypteret sikkert print	Forøg beskyttelsen af Sikkert print ved at kryptere filen og adgangskoden under overførslen	Konfigurér brugernavnet under fanen Printer i klientprinterkonfigurationen til et andet brugernavn end LDAP-/domænelegitimationsoplysningerne for den pågældende bruger. Sørg for, at "Restrict printer jobs" (Begræns printerjob) er slået fra
Automatisk certifikatregistrering	Den automatiske registreringsproces forbedrer effektiviteten af hentning og implementering af digital certificering	Kræver en netværkscertifikatløsning for at kunne anvendes
Syslog-hændelsesnotifikation	Systemlogprotokollen er en standardindustriprotokol, der bruges til at sende systemlog- eller hændelsesmeddelelser til en bestemt server, der kaldes en Syslog-server	Overvej at henvise imageRUNNER ADVANCE-Syslog-dataene til jeres eksisterende netværks systemlog-analyseværktøj eller SIEM-platform (Enterprise Security Event Management System)
Bekræft system ved opstart	Giver sikkerhed for, at systemets softwarekomponenter ikke er blevet kompromitteret. Det vil have en minimal indvirkning på systemets opstartstid	Aktivér funktionen
Trådløst LAN	Giver trådløs adgang	Brug WPA-PSK/WPA2-PSK med stærke adgangskoder
WiFi Direct	Bruges til at oprette en Wi-Fi Direct-forbindelse	Deaktivér Wi-Fi Direct
Integreret webbrowser (tilgængelig fra Generation 3-modeller, 2. udgave)	Browseradgang til internettet	Anvend passende begrænsninger, eller deaktivér muligheden for at downloade filer, der er hentet via en browser

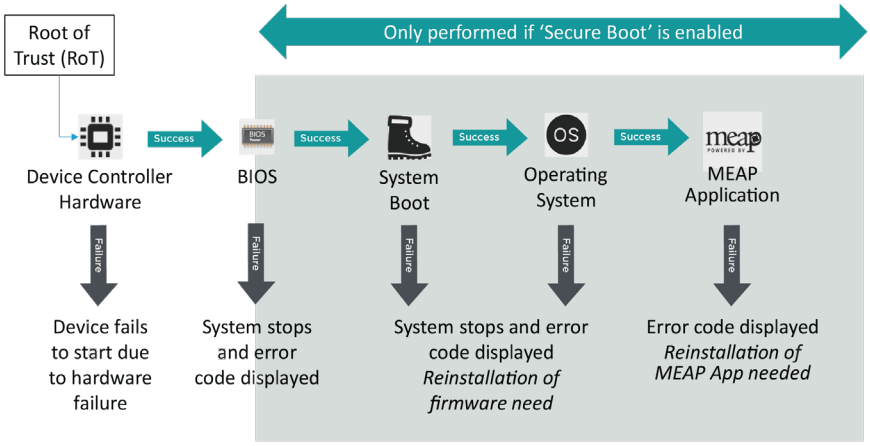
Den nyeste generation af imageRUNNER ADVANCE-modeller har trådløs netværksforbindelse, så enheden kan oprette forbindelse til et Wi-Fi-netværk, samtidig med at den er tilsluttet et kabelforbundet netværk. Dette scenarie kan være nyttigt, når kunden har brug for at dele en enhed på tværs af to netværk. Et skolemiljø er et typisk eksempel, hvor der er separate medarbejder- og elevnetværk.

imageRUNNER ADVANCE-platformen giver et funktionsmiljø, som kan bruges på en fleksibel måde. Med de protokoller og tjenester, der er tilgængelige for at opnå dette, er det vigtigt at sikre, at kun de nødvendige funktioner, tjenester og protokoller er aktiveret for at opfylde brugerens behov. Dette er god sikkerhedspraksis og vil reducere den potentielle angrebsoverflade og forhindre misbrug af disse. Da der hele tiden dukker nye sårbarheder op, skal vi altid være opmærksomme på, om enheden udsættes for farer, både internt og eksternt. Muligheden for at overvåge brugeraktiviteten er nyttig til at hjælpe med at identificere og foretage korrigerende handlinger, når det er nødvendigt.

imageRUNNER ADVANCE-softwareplatform version 3.8 indeholder nogle ekstra funktioner ud over dem, der har været tilgængelige i en årrække. Disse omfatter muligheden for at overvåge enheden i realtid ved hjælp af Syslog og 'Bekræft system ved opstart'. Brug af disse funktioner sammen med jeres eksisterende netværkssikkerhedsløsninger, f.eks. en SIEM-platform (Security Information Event Management) eller logningsløsning, giver mulighed for større synlighed og identifikation af hændelser og til kriminaltekniske formål.

Bekræft system ved opstart

Denne funktionalitet er en hardwaremekanisme, der er designet til at sikre, at alle dele af imageRUNNER ADVANCE generation 3-systemsoftwaren, 3. udgave, verificeres i forhold til en Root of Trust for at sikre, at operativsystemet indlæses, som det er tilsigtet af Canon. Hvis en ondsindet part manipulerer eller prøver at ændre systemet, eller hvis der opstår en fejl under indlæsning af systemet, stopper processen, og der vises en fejlkode.



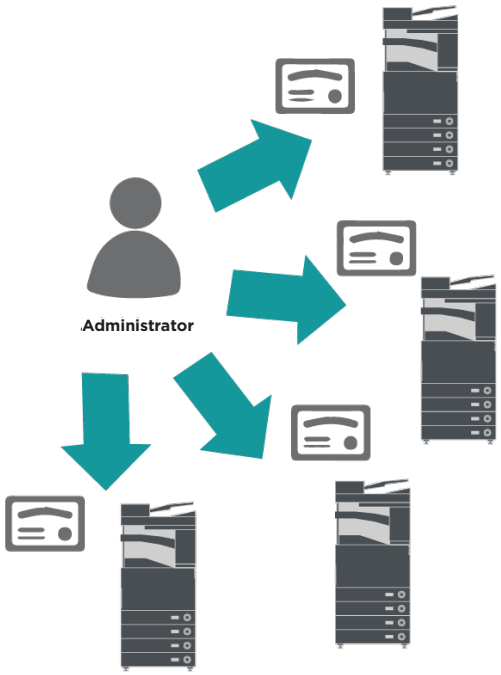
Figur 3 Proces for 'Bekræft system ved opstart'

Denne proces er synlig for brugeren bortset fra, at displayet angiver, at der indlæses en utilsigtet systemversion. imageRUNNER ADVANCE generation 3, 3. udgave, har en funktion til at aktivere 'Bekræft system ved opstart', som skal aktiveres for at aktivere denne sikkerhedsfunktion.

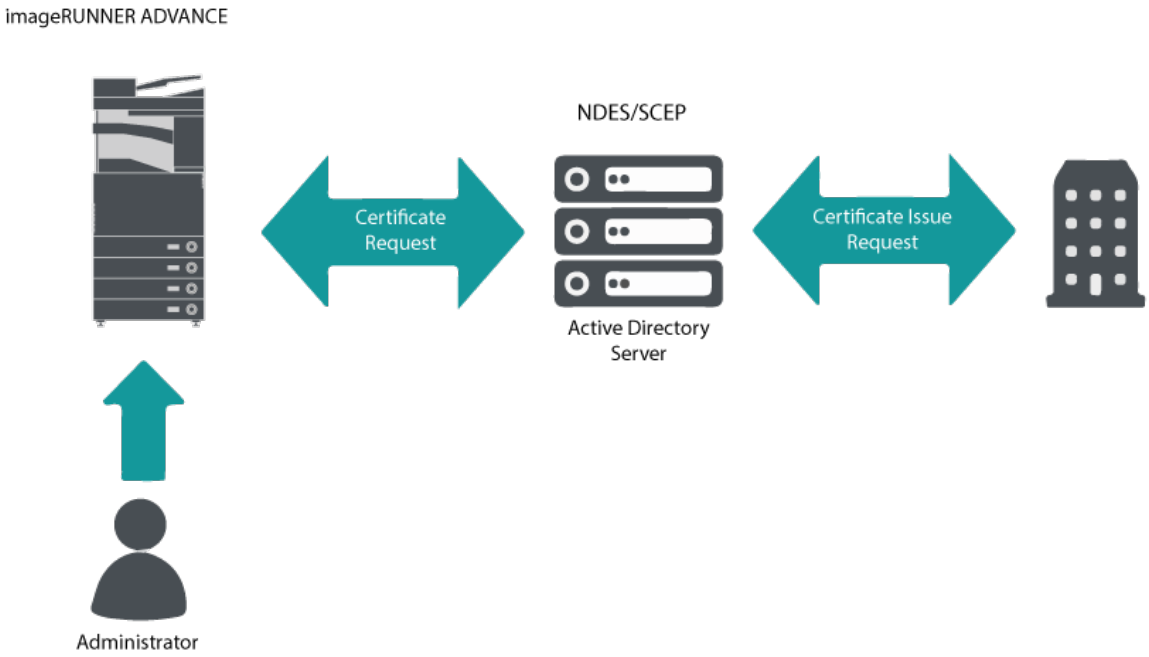
Automatisk certifikatregistrering

I versioner af imageRUNNER ADVANCE-systemsoftwareplatformen før version 3.8 var administratoren nødt til manuelt at installere opdaterede sikkerhedscertifikater på hver enhed.
Dette er en krævende opgave, da der er behov for at oprette forbindelse til hver enkelt enhed skiftevis for at udføre en manuel opdatering – certifikater skal installeres manuelt ved hjælp af det specifikke fjernbrugerinterface (Remote UI), hvilket gør processen meget mere tidskrævende. Med tjenesten til automatisk certifikatregistrering, der introduceres fra platform version 3.8 og derover, er denne omkostning blevet elimineret.

Den automatiske registreringsproces forbedrer effektiviteten af certifikathentningen. Den giver mulighed for automatisk at hente certifikater ved hjælp af NDES (Network Device Enrolment Service) til Microsoft Windows og SCEP (Simple Certificate Enrolment Protocol).



Figur 4 Certifikatregistrering



Figur 5 Certifikatregistreringsproces

SCEP er en protokol, der understøtter certifikater udstedt af en certifikatmyndighed, og NDES gør det muligt for netværksenheder at hente eller opdatere certifikater baseret på SCEP.

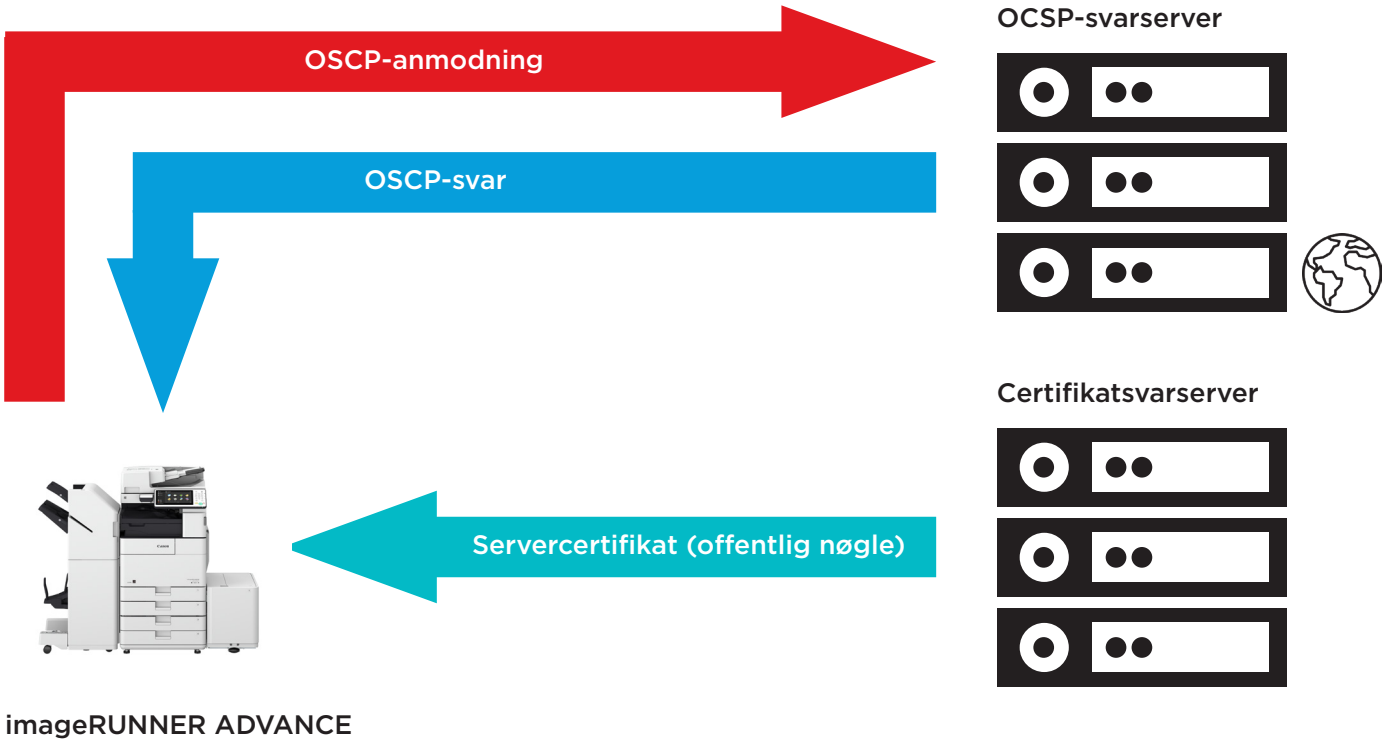
NDES er en vigtig tjeneste i Active Directory-certifikattjenester.

OCSP (Online Certificate Status Protocol)

Der er en række grunde til, at det kan være nødvendigt at tilbagekalde et digitalt certifikat. Eksempler på dette kan være, at den private nøgle er gået tabt, blevet stjålet eller kompromitteret, eller at et domænenavn er blevet ændret.

OCSP (Online Certificate Status Protocol) er en standardinternetprotokol, der bruges til at kontrollere tilbagetrækningsstatus for et digitalt X.509-certifikat, der er leveret af certifikatserveren. Ved at sende en OCSP-anmodning til OCSP-svarserveren (typisk en certifikatudsteder) med angivelse af et specifikt certifikat, vil OCSP-svarserveren svare med "good" (godkendt), "revoked" (tilbagekaldt) eller "unknown" (ukendt).

Figur 6 OCSP-håndtryksproces



Med imageRUNNER ADVANCE fra platform version 3.10 leverer OCSP en mekanisme i realtid til at kontrollere de installerede digitale X.509-certifikater. Tidligere versioner af platformen understøttede kun CRL-metoden (Certificate Revoke List), som er ineffektiv og resulterer i store omkostninger til netværksressourcer.

Sikkerhedsoplysninger og hændelsesstyring

imageRUNNER ADVANCE-teknologien understøtter muligheden for at udsende sikkerhedshændelser i realtid ved hjælp af Syslog-protokollen, som overholder RFC 5424, RFC 5425 og RFC 5426.

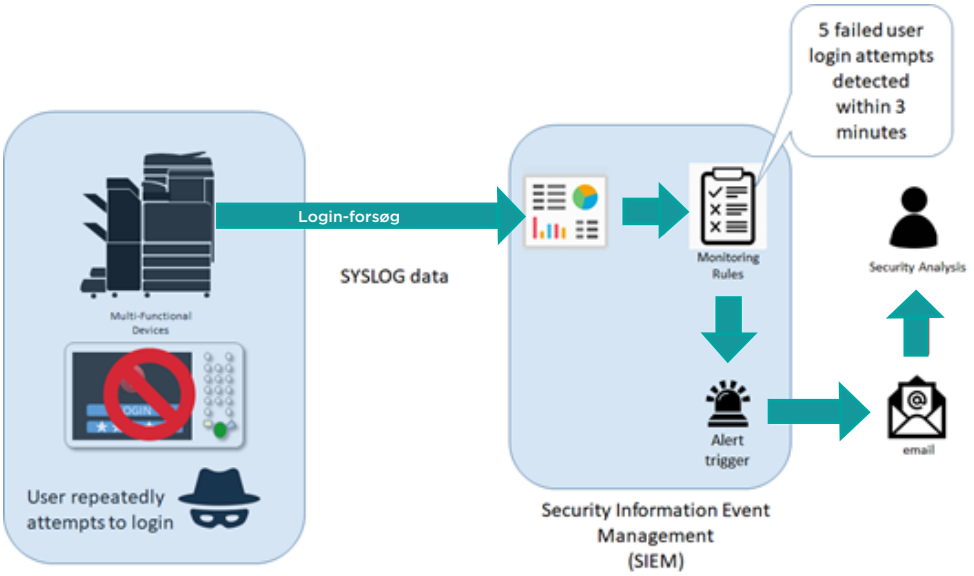
Denne protokol bruges af en lang række enhedstyper som en metode til at indsamle oplysninger i realtid, der kan bruges til at identificere potentielle sikkerhedsproblemer.

For at gøre det lettere at opdage trusler og sikkerhedshændelser skal MFP'en konfigureres til at pege på en SIEM-server (Security Incident Event Management) fra en tredjepart.

Syslog-hændelser, der fremstilles af MFP'en, kan bruges til at oprette handlinger via indsamling og analyse i realtid af hændelser fra en lang række kontekstuelle datakilder (Figur 7). De kan også understøtte rapportering af overholdelse og undersøgelse af hændelser ved hjælp af yderligere løsninger som f.eks. en SIEM-server. Et eksempel kan ses i Figur 8.

Den nyeste generation af imageRUNNER ADVANCE-enheder indeholder Syslog-funktionalitet, der understøtter en række hændelser, som kan indsamles. Dette kan bruges til at sammenholde og analysere hændelser på tværs af en række forskellige kilder for at identificere udviklinger eller abnormiteter.

Figur 7 Syslog-dataindsamling



Figur 8 Eksempel på brug af imageRUNNER ADVANCE Syslog-data

Administration af enhedslogfiler

Ud over Syslog-funktionaliteten, som er tilgængelig fra systemsoftwareplatform version 3.8, har imageRUNNER ADVANCE følgende logfiler, der kan administreres på enheden. Disse logfiler kan eksporteres i CSV-filformat via fjernbrugerinterfacet (RUI).

Tabel 3 – Eksempler på logfiler, der kan administreres af multifunktionsprinteren.

Logtype	Tallet, der er angivet som "Log Type" i CSV-filen	Beskrivelse
Log	4098	Denne log indeholder oplysninger om godkendelsesstatus for brugergodkendelse (login/logout og fuldført/mislykket brugergodkendelse), registrering/ændring/sletning af brugeroplysninger, der administreres med brugergodkendelse, og administration (tilføjelse/redigering/sletning) af roller med ACCESS MANAGEMENT SYSTEM (Adgangskontrolsystem)
Joblog	1001	Denne log indeholder oplysninger om fuldførelse af kopierings-/fax-/scannings-/afsendelses-/printjob
Overførselslog	8193	Loggen indeholder oplysninger om overførsler
Advanced Space-lagringslog	8196	Denne log indeholder oplysninger om lagring af filer på Advanced Space, netværket (Advanced Space på andre maskiner) og hukommelsesmedier
Log for mailbokshandlinger	8197	Denne log indeholder oplysninger om de handlinger, der udføres på data i mailboksen, Memory RX-indbakken og Confidential Fax-indbakken
Log for mailboksgodkendelse	8199	Denne log indeholder oplysninger om godkendelsesstatus for mailboksen, Memory RX-indbakken og Confidential Fax-indbakken
Log for Advanced Space-handlinger	8201	Denne log indeholder oplysninger om datahandlinger i Advanced Space
Log for maskinadministration	8198	Denne log indeholder oplysninger om start/nedlukning af maskinen, ændringer foretaget i indstillingerne ved hjælp af Settings/Registration (Indstillinger/registrering), ændringer foretaget i indstillingerne ved hjælp af funktionen Device Information Delivery (Levering af enhedsoplysninger) og tidsindstillingen. Logfilen for maskinadministration registrerer også ændringer i brugeroplysninger eller sikkerhedsrelaterede indstillinger, når maskinen efterses eller repareres af din lokale autoriserede Canon-forhandler
Log for netværksgodkendelse	8200	Denne log registreres, når IPSec-kommunikation mislykkes
Log for Eksportér/importér alle	8202	Denne log indeholder oplysninger om import/eksport af indstillingerne ved hjælp af funktionen Export All/Import All (Eksportér alle/importér alle)
Log for sikkerhedskopiering af mailboks	8203	Denne log indeholder oplysninger om sikkerhedskopiering af data i brugerindbakkerne, Memory RX-indbakken, Confidential Fax-indbakken, Advanced Space og eventuelle indeholdte data samt den formular, der er registreret til funktionen Superimpose Images (Overlejr billeder)
Log for handlinger på skærmen til program-/softwarestyring	3101	Dette er en handlingslog for SMS (Service Management Service), softwareregistrering/-opdateringer og MEAP-programinstallationsværktøjer osv.
Log for sikkerhedspolitik	8204	Denne log indeholder oplysninger om indstillingsstatus for sikkerhedspolitikindstillingerne
Log for gruppeadministration	8205	Denne log indeholder oplysninger om indstillingsstatus (registrering/redigering/sletning) for brugergrupperne
Log for systemvedligeholdelse	8206	Denne log indeholder oplysninger om firmwareopdateringer og sikkerhedskopiering/gendannelse af MEAP-programmet osv.
Log for printgodkendelse	8207	Denne log indeholder oplysninger og handlingshistorik vedrørende printjob med tvunget tilbageholdelse
Log for synkronisering af indstillinger	8208	Denne log indeholder oplysninger om synkronisering af maskinindstillinger. Synkronisering af indstillinger for flere Canon-multifunktionsprintere
Log for administration af overvågningslog	3001	Denne log indeholder oplysninger om start og slut af denne funktion (funktionen Audit Log Management (Administration af overvågningslog)) samt eksport af logfiler osv.

Logfiler kan indeholde op til 40.000 poster. Når antallet af poster overstiger 40.000, slettes de ældste poster først.

UNDERSTØTTELSE AF EKSTERN ENHED

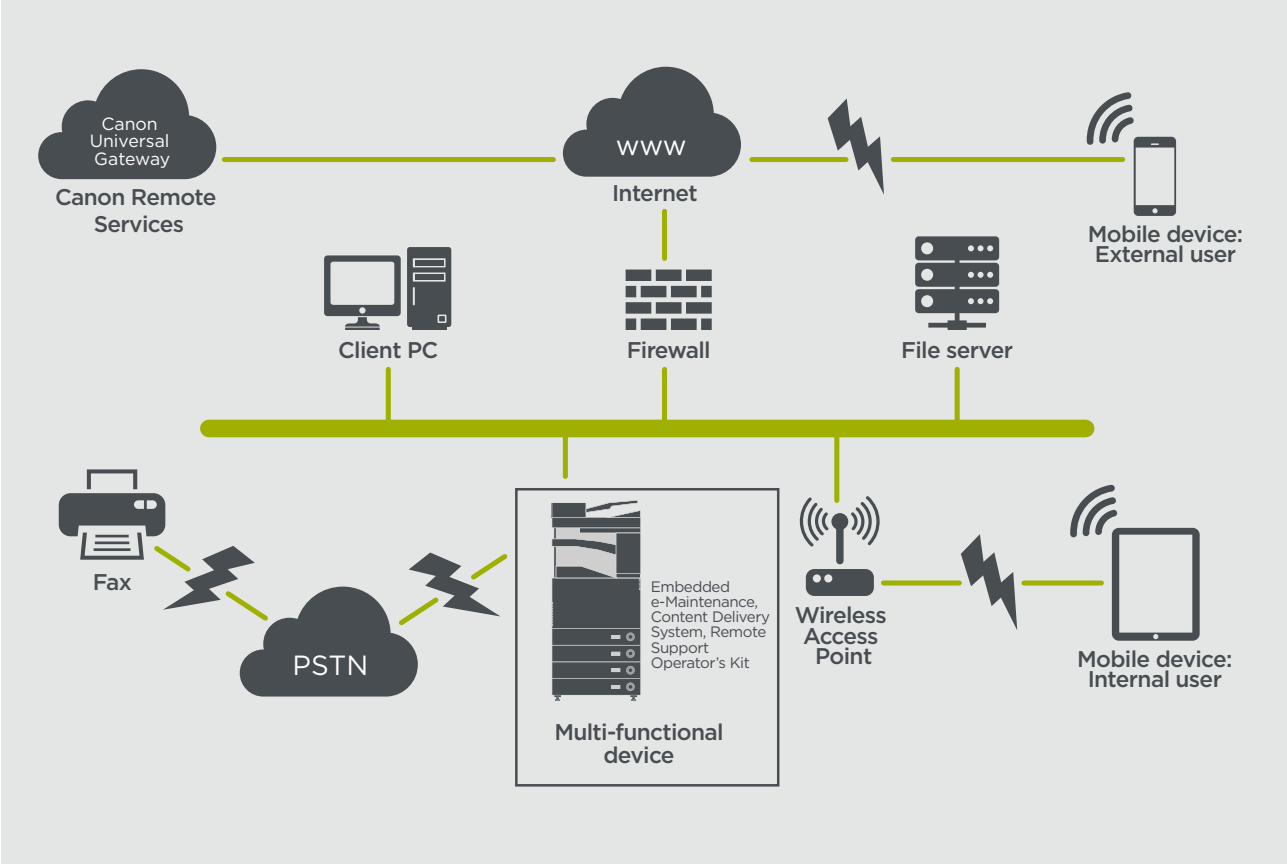
For at Canon eller en Canon-partner kan yde effektiv service, kan imageRUNNER ADVANCE sende servicerelaterede data samt modtage firmwareopdateringer eller softwareprogrammer. Det skal bemærkes, at der ikke sendes billeder eller metadata om billeder.

Nedenfor vises to mulige implementeringer af Canons fjerntjenester i et virksomhedsnetværk.

Implementeringsscenarie 1: Spredt forbindelse

I denne indstilling giver hver multifunktionsprinter mulighed for direkte forbindelse til fjerntjenesten via internettet.

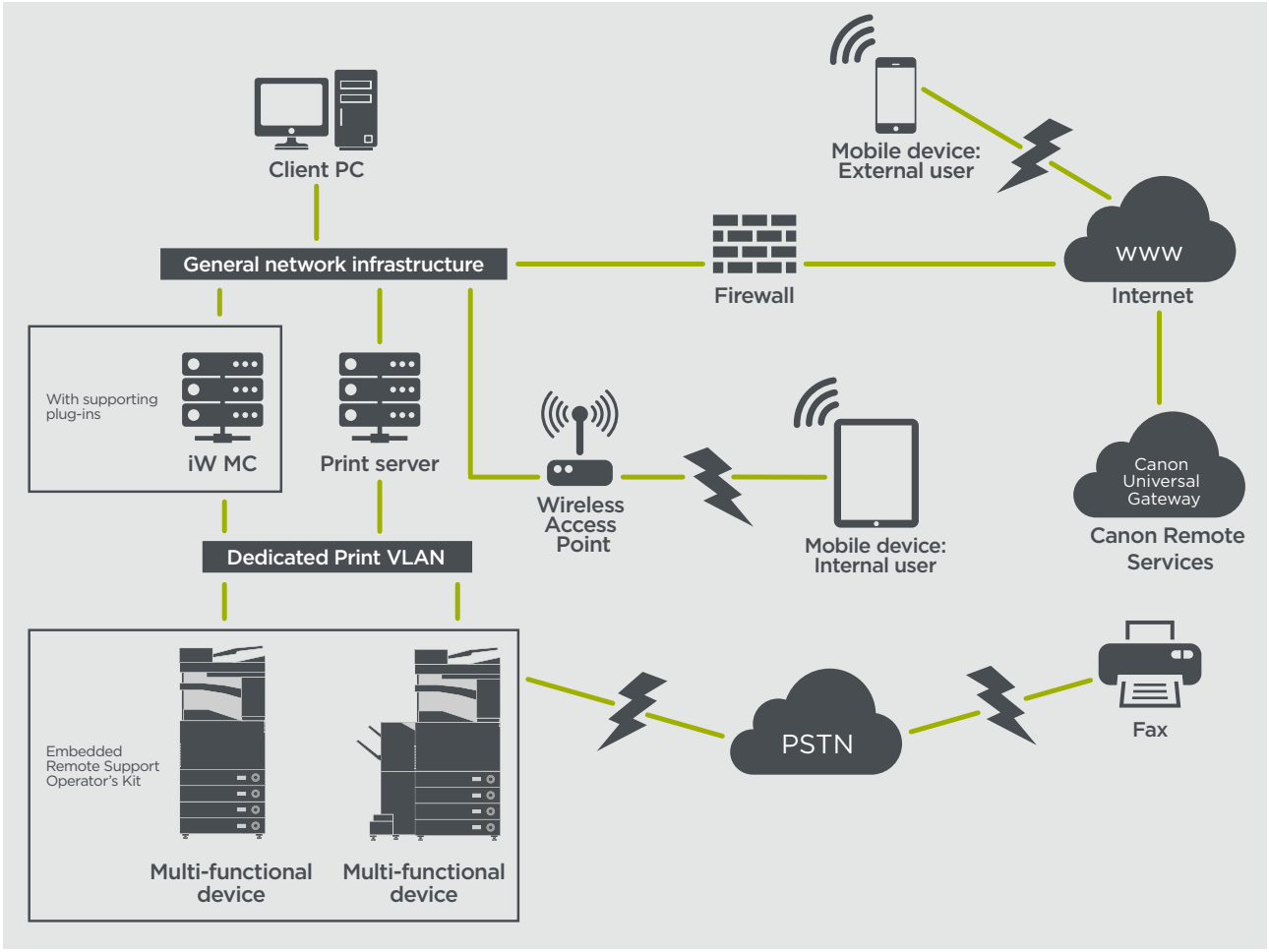
Figur 9 Spredt forbindelse



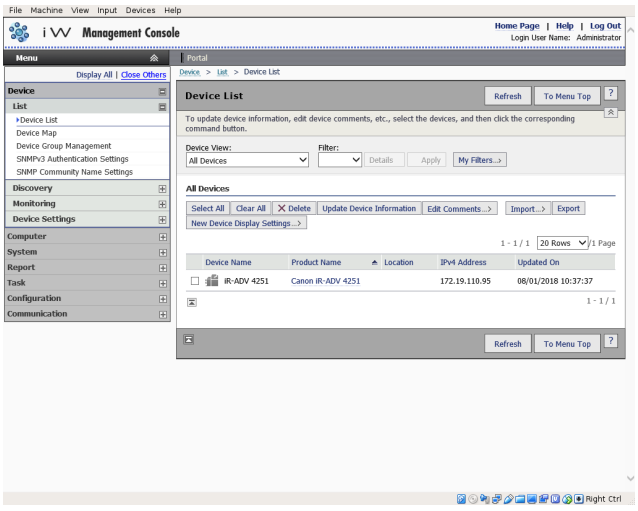
Implementeringsscenarie 2: Centraliseret administreret forbindelse

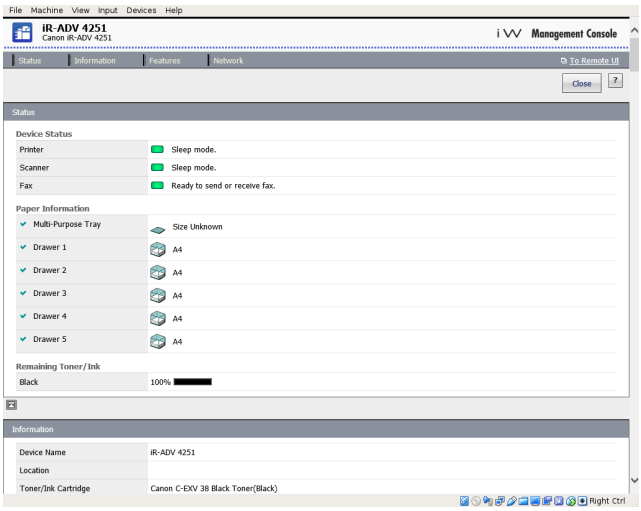
I et virksomhedsmiljø, hvor der er installeret flere multifunktionsprintere, er der behov for at kunne administrere disse enheder effektivt fra ét centralt punkt, og det omfatter forbindelsen til Canons fjerntjenester. For at forenkle den helhedsorienterede administrationstilgang opretter de enkelte enheder administrationsforbindelser via et enkelt iWMC-forbindelsespunkt (iW Management Console). Til kommunikation mellem DFU-plug-in'en (Device Firmware Upgrade) og multifunktionsprintere anvendes UDP-port 47545.

Figur 10 Centraliseret administreret forbindelse



Figur
11a. Enhedsliste (i dette tilfælde en enkelt enhed) som rapporteret på iWMC (imageWARE Management Console) og
11b. Enhedsoplysninger og -indstillinger





Figur 11a **Figur 11b**

e-Maintenance

e-Maintenance-systemet giver en automatisk metode til indsamling af tællere for enhedsbrug til faktureringsformål, styring af forbrugsstoffer og overvågning af eksterne enheder via status- og fejlmeddelelser.

e-Maintenance-systemet består af en internetrettet server (UGW) og enten en integreret software til multifunktionsenheder (eRDS) og/eller ekstra serverbaseret software (RDS-plug-in) til at indsamle oplysninger om enhedstjenester. eRDS er et overvågningsprogram, der kører internt i imageRUNNER ADVANCE. Hvis overvågningsfunktionen er aktiveret i enhedens indstillinger, henter eRDS sine egne enhedsoplysninger og sender dem til UGW. RDS-plug-in'en er et overvågningsprogram, der er installeret på en almindelig pc, og som kan overvåge 1 til 3.000 enheder. Det indhenter oplysninger fra hver enhed via netværket og sender dem til UGW.

Som vist i tabel 4 nedenfor viser den næste side en oversigt over de overførte data, protokoller (afhænger af de indstillinger, der blev valgt under design og implementering) og anvendte porte. Der overføres på intet tidspunkt billeddata fra kopiering, print, scanning eller fax.

Tabel 4 Oversigt over eMaintenance-data

Beskrivelse	Håndteret data	Protokol/port	Port
Kommunikation mellem eMaintenance (eRDS- eller RDS-plug-in) og UGW	UGW-webtjenesteadresse Proxy-serveradresse/-portnummer Proxy-konto/-adgangskode UGW-maildestinationsadresse SMTP-serveradresse POP-serveradresse Enhedsstatus, tæller og modeloplysninger Serienummer Oplysninger om resterende toner/blæk Firmwareoplysninger Oplysninger om reparationsanmodning Logoplysninger Serviceopkald Servicealarm Papirstop Miljø Betingelseslog	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Kommunikation mellem eMaintenance og MFP (kun RDS-plug-in, da eRDS er integreret software)		SNMP Canon-navnebeskyttet SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Content Delivery System

CDS (Content Delivery System) opretter en forbindelse mellem multifunktionsprinteren og Canon Universal Gateway (UGW). Det leverer enhedsfirmware- og programopdateringer.

Tabel 5 Oversigt over Content Delivery System-data

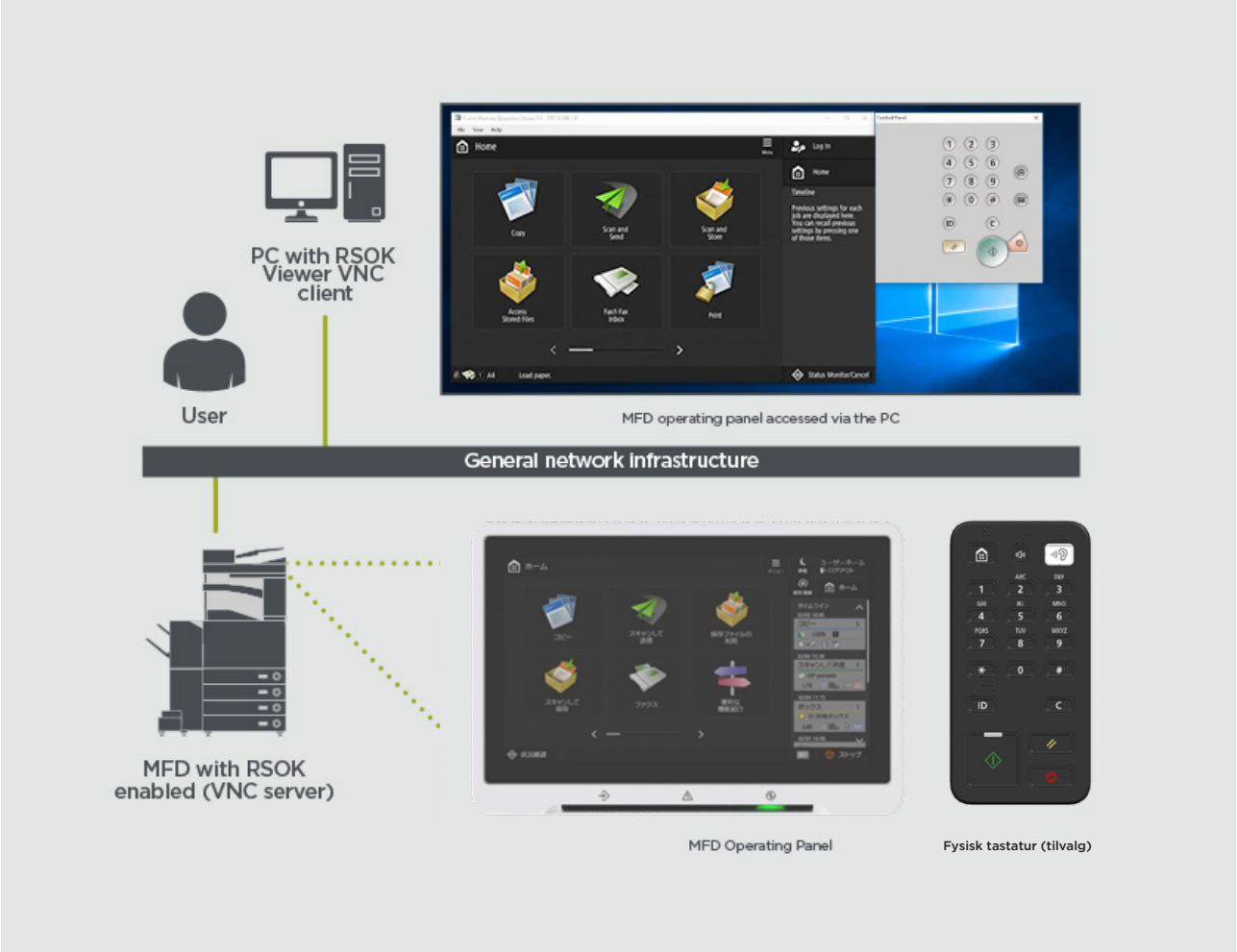
Beskrivelse	Data sendt	Protokol/port	Port
Kommunikation mellem multifunktionsprinter og UGW	Enhedens serienummer Firmwareversion Sprog Land Oplysninger vedrørende slutbrugerlicensaftalen for enheden	HTTP/HTTPS	TCP/80 TCP/443
Kommunikation mellem UGW og multifunktionsprinter	Testfil (binære tilfældige data) til kommunikationstest Binære data i firmwaren eller MEAP-programmet	HTTP/HTTPS	TCP/80 TCP/443

En specifik URL til CDS-adgang er forudindstillet i enhedskonfigurationen.
Hvis der er behov for centraliseret enhedsfirmware- og programstyring i infrastrukturen, kræves en lokal installation af iWMC med DFU-plug-in (Device Firmware Upgrade) og plug-in til enhedsprogramadministration.

RSOK (Remote Support Operator's Kit)

RSOK (Remote Support Operator's Kit): Giver fjernadgang til enhedens kontrolpanel. Dette system af serverklienttypen består af en VNC-server, der kører på multifunktionsprinteren, og Microsoft Windows-klientprogrammet Remote Operation Viewer VNC.

Figur 12 Opsætning af RSOK (Remote Support Operator's Kit)



Tabel Dataoversigt for RSOK (Remote Support Operator's Kit)

Beskrivelse	Data sendt	Protokol/port	Port
VNC-adgangskodegodkendelse	Brugeradgangskode	DES-kryptering	5900
Handlingsvisning	Enhedskontrolpanel - skærmdata - betjening af hardwarenøglen	Version 3.3 RFB-protokol	5900

APPENDIKS

Canon imageRUNNER ADVANCE – sikkerhedsrelaterede funktioner

imageRUNNER ADVANCE-platformen giver mulighed for fjernkonfiguration via et webtjenesteinterface, der kaldes RUI (Remote User Interface). Dette interface giver adgang til mange af enhedens konfigurationsindstillinger og kan deaktiveres, hvis dette ikke er tilladt. Det beskyttes med en adgangskode for at forhindre uautoriseret adgang.

Mens de fleste enhedsindstillinger er tilgængelige via RUI, er det nødvendigt at bruge enhedens kontrolpanel til at indstille elementer, som ikke kan indstilles ved hjælp af dette interface. Vi anbefaler, at du deaktiverer alle ubrugte tjenester og strammer kontrollerne op på dem, der er brug for. For at give fleksibilitet og support giver RSOK (Remote Service Operator's Kit) fjernadgang til enhedens kontrolpanel. Dette er baseret på VNC-teknologi, der består af en server (multifunktionsprinteren) og en klient (en netværks-pc). Der findes en specifik klient-pc-fremviser fra Canon, som giver simuleret adgang til kontrolpanelets taster, hvor det er nødvendigt.

Dette afsnit giver en oversigt over de vigtigste sikkerhedsrelaterede imageRUNNER ADVANCE-funktioner og deres konfigurationsindstillinger.

Interaktive online brugermanualer er tilgængelige på https://oip.manual.canon/ og indeholder oplysninger, der ikke kun dækker sikkerhedsrelaterede funktioner. Start med at vælge den relevante produkttype (f.eks. imageRUNNER ADVANCE DX), klik på søgeikonet, og indtast dine søgekriterier. Nedenfor er et par generelle områder, der er værd at overveje.

Administration af maskinen

For at reducere lækage af personlige oplysninger eller uautoriseret brug er det nødvendigt med konstante og effektive sikkerhedsforanstaltninger. Ved at udpege en administrator til at håndtere enhedsindstillinger kan brugeradministration og sikkerhedsindstillinger begrænses udelukkende til autoriserede personer.

Brug nedenstående link i din webbrowser, og indtast **administrator configuration** (administratorkonfiguration) i søgefeltet. Dette vil give oplysninger om:

- Grundlæggende administration af enheden
- Begrænsning af risici som følge af uagtsomhed, brugerfejl og misbrug
- Enhedsstyring
- Administration af systemkonfiguration og -indstillinger

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

IEEE P2600-standard

En række imageRUNNER ADVANCE-modeller er IEEE P2600-kompatible, hvilket er en global informationssikkerhedsstandard for eksterne multifunktionsenheder og printere.

Linket nedenfor beskriver de sikkerhedskrav, der er defineret i IEEE 2600-standarden, og hvordan enhedens funktioner opfylder disse krav.

http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

IEEE 802.1X-godkendelse

Når der er behov for at oprette forbindelse til et 802.1X-netværk, skal enheden godkendes for at sikre, at det er en autoriseret forbindelse.

Brug nedenstående link i din webbrowser, og indtast **802.1X** i søgefeltet.

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

Anvendelse af en sikkerhedspolitik på maskinen

De nyeste imageRUNNER ADVANCE-modeller giver mulighed for, at flere sikkerhedsindstillinger for printeren, sikkerhedspolitikken, kan administreres samlet via RUI. Der kan bruges en separat adgangskode, der kun tillader sikkerhedsadministratoren at ændre indstillingerne.

Brug nedenstående link i din webbrowser, og indtast **Applying a Security Policy to the Machine** (Anvendelse af en sikkerhedspolitik på maskinen) i søgefeltet. Dette vil give oplysninger om:

- Brug af en adgangskode til at beskytte indstillingerne for sikkerhedspolitikken
- Konfiguration af indstillingerne for sikkerhedspolitikken
- Elementer i indstillingerne for sikkerhedspolitikken

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

Administration af brugere

Kunder, der har behov for et højere niveau af sikkerhed og effektivitet, kan enten bruge en indbygget funktionalitet eller bruge en print management-løsning, f.eks. uniFLOW.

Kontakt vores lokale repræsentant for yderligere information om vores printhåndteringsløsninger, eller se uniFLOW-produktbrochuren.

Konfiguration af netværkssikkerhedsindstillingerne

Autoriserede brugere kan pådrage sig uventede tab som følge af angreb fra ondsindede tredjeparter, f.eks. sniffing, spoofing og manipulation af data, når de sendes over et netværk. For at beskytte jeres vigtige og værdifulde data mod disse angreb understøtter maskinen adskillige funktioner, der forbedrer sikkerheden og beskyttelsen af personlige oplysninger.

Brug nedenstående link i din webbrowser, og indtast **Configuring the Network Security Settings** (Konfiguration af netværkssikkerhedsindstillingerne) i søgefeltet. Dette vil give oplysninger om:

Linket nedenfor indeholder oplysninger om:

- Hindring af uautoriseret adgang
- Oprettelse af forbindelse til et trådløst LAN
- Opsætning af netværksmiljøet

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

Håndtering af harddiskdata

Printerens harddisk bruges til at gemme printerens operativsystem, konfigurationsindstillinger og joboplysninger. De fleste modeller har fuld diskkryptering (i overensstemmelse med FIPS 140-2) ved at parre den med den specifikke enhed, så den ikke kan læses af uautoriserede brugere. En forberedende sikkerhedschip til Canon-multifunktionsprintere er certificeret som et kryptografisk modul under CMVP (Cryptographic Module Validation Program), der er oprettet af USA og Canada, samt JCMVP (Japan Cryptographic Module Validation Program).

Brug nedenstående link i din webbrowser, og indtast **Managing Hard Disk Data** (Håndtering af harddiskdata) i søgefeltet.

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

OVERSIGT OVER INDSTILLINGER FOR SIKKERHEDSPOLITIK

Tredje generation af imageRUNNER ADVANCE-modellerne introducerer indstillinger for sikkerhedspolitik og mulighed for at udpege en sikkerhedsadministrationsbruger. Dette kræver, at administratoren er logget på, og, hvis det er konfigureret, et yderligere sikkerhedsadministratorlogin med en ekstra adgangskode.

Tabellen nedenfor viser de tilgængelige indstillinger.

1. Interface	Bemærkninger
Politik for trådløs forbindelse	
Forbyd brug af direkte forbindelse	<Use Wi-Fi Direct> (Brug Wi-Fi Direct) er indstillet til <Off> (Fra) Det er ikke muligt at få adgang til maskinen fra mobile enheder
Forbyd brug af trådløst LAN	<Select Wired/Wireless LAN> (Vælg kabelforbundet/trådløst LAN) er indstillet til <Wired LAN> (Kabelforbundet LAN) Det er ikke muligt at oprette en trådløs forbindelse til maskinen via en trådløs LAN-router eller et trådløst adgangspunkt
USB-politik	
Forbyd brug som USB-enhed	<Use as USB Device> (Brug som USB-enhed) er indstillet til <Off> (Fra) Du vil ikke kunne bruge print- eller scanningsfunktionerne fra pc'er, der er tilsluttet via USB, når Brug som USB-enhed er forbudt
Forbyd brug som USB-lagerenhed	<Use USB Storage Device> (Brug USB-lagerenhed) er indstillet til <Off> (Fra) Det er ikke muligt at bruge USB-lagerenheder Følgende servicefunktioner virker dog stadig, selvom "Prohibit use as USB storage device" (Forbyd brug som USB-lagerenhed) er aktiveret • Firmwareopdatering via USB-nøgle (fra downloadfunktion) • Kopiering af underlog-data fra enheden til USB (LOG2USB) • Kopiering af rapporten fra enheden til USB (RPT2USB)
Driftspolitik for netværkskommunikation Bemærk: Disse indstillinger gælder ikke for kommunikation med IEEE 802.1X-netværk, selvom afkrydsningsfeltet er markeret for [Always Verify Server Certificate When Using TLS] (Verificér altid servercertifikat ved brug af TLS)	
Verificér altid signaturer for SMS/ WebDAV-serverfunktioner	I <SMB Server Settings> (SMB-serverindstillinger) er indstillingerne <Require SMB Signature for Connection> (Kræv SMB-signatur ved forbindelse) og <Use SMB Authentication> (Brug SMB-godkendelse) indstillet til <On> (Til), og <Use TLS> (Brug TLS) i <WebDAV Server Settings> (WebDAV-serverindstillinger) er indstillet til <On> (Til) Når maskinen bruges som SMB-server eller WebDAV-server, verificeres digitale certifikatsignaturer under kommunikationen
Verificér altid servercertifikat ved brug af TLS	<Confirm TLS Certificate for WebDAV TX> (Bekræft TLS-certifikat for WebDAV TX), <Confirm TLS Certificate for SMTP TX> (Bekræft TLS-certifikat for SMTP TX), <Confirm TLS Certificate for Network Access> (Bekræft TLS-certifikat for netværksadgang) og <Confirm TLS Certificate Using MEAP Application> (Bekræft TLS-certifikat ved brug af MEAP-program) er alle indstillet til <On> (Til), og der sættes et flueben ved <CN> Desuden er indstillingerne <Verify Server Certificate> (Verificér servercertifikat) og <Verify CN> (Verificér CN) i <SIP Settings> (SIP-indstillinger) > <TLS Settings> (TLS-indstillinger) indstillet til <On> (Til) Under TLS-kommunikation udføres kontrol af digitale certifikater og deres almindelige navne
Forbyd klar tekst-godkendelse for serverfunktioner	• <Use FTP Printing> (Brug FTP-print) i <FTP Print Settings> (FTP-printindstillinger) er indstillet til <Off> (Fra) • <Allow TLS (SMTP RX)> (Tillad TLS (SMTP RX)) i <E-Mail/I-Fax Settings> (Indstillinger for e-mail/I-Fax) <Communication Settings> (Kommunikationsindstillinger) er indstillet til <Always TLS> (Altid TLS), <Dedicated Port Authentication Method> (Dedikeret portgodkendelsesmetode) i <Network> (Netværk) er indstillet til <Mode 2> (Metode 2), • <Use TLS> (Brug TLS) i <WebDAV Server Settings> (WebDAV-serverindstillinger)> er indstillet til <On> (Til) Når maskinen bruges som server, er funktioner, der bruger godkendelse med almindelig tekst, ikke tilgængelige TLS anvendes, hvis klar tekst-godkendelse er forbudt. Desuden vil du ikke kunne bruge programmer eller serverfunktioner som f.eks. FTP, der kun understøtter godkendelse med klar tekst Det er muligvis ikke muligt at få adgang til maskinen fra enhedsstyringssoftware eller -driver
Forbyd brug af SNMPv1	I <SNMP Settings> (SNMP-indstillinger) er <Use SNMPv1> (Brug SNMPv1) indstillet til <Off> (Fra) Du kan muligvis ikke hente eller indstille enhedsoplysningerne fra printerdriveren eller administrationssoftwaren, hvis brugen af SNMPv1 er forbudt
Politik for brug af porte	
Begræns LPD-port	Portnummer: 515 <LPD Print Settings> (LPD-printindstillinger) er indstillet til <Off> (Fra) Det er ikke muligt at udføre LPD-print
Begræns RAW-port	Portnummer 9100 <RAW Print Settings> (RAW-printindstillinger) er indstillet til <Off> (Fra) Det er ikke muligt at udføre RAW-print
Begræns FTP-port	Portnummer 21 I <FTP Print Settings> (FTP-printindstillinger) er <Use FTP Printing> (Brug FTP-print) indstillet til <Off> (Fra) Det er ikke muligt at udføre FTP-print
Begræns WSD-port	Portnummer 3702, 60000 I <WSD Settings> (WSD-indstillinger) er indstillingerne <Use WSD> (Brug WSD), <Use WSD Browsing> (Brug WSD-browsing) og <Use WSD Scan> (Brug WSD-scanning) alle indstillet til <Off> (Fra) Det er ikke muligt at bruge WSD-funktioner
Begræns BMLinkS-port	Portnummer 1900 Anvendes ikke i den europæiske region
Begræns IPP-port	Portnummer 631 Du vil ikke kunne bruge Mopria, AirPrint og IPP, hvis IPP-porten er begrænset

Begræns SMB-port	Portnummer: 137, 138, 139, 445 I <SMB Server Settings> (SMB-serverindstillinger) er <Use SMB Server> (Brug SMB-server) indstillet til <Off> (Fra) Det er ikke muligt at bruge maskinen som SMB-server
Begræns SMTP-port	Portnummer 25 I <E-Mail/I-Fax Settings> (Indstillinger for e-mail/I-Fax) > <Communication Settings> (Kommunikationsindstillinger) er <SMTP RX> indstillet til <Off> (Fra) SMTP-modtagelse er ikke muligt
Begræns dedikeret port	Portnummer: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545-47547 I vil ikke kunne bruge funktionerne til fjernkopiering, -fax, -scanning eller -print og heller ikke programmer osv., hvis den dedikerede port er begrænset
Begræns fjernoperatørens softwareport	Portnummer 5900 <Remote Operation Settings> (Indstillinger for fjernbetjening) er indstillet til <Off> (Fra) Det er ikke muligt at bruge fjernbetjeningsfunktioner
Begræns SIP-port (IP Fax)	Portnummer: 5004, 5005, 5060, 5061, 49152 <Use Intranet> (Brug intranet) i <Intranet Settings> (Intranet-indstillinger), <Use NGN> (Brug NGN) i <NGN Settings> (NGN-indstillinger) og <Use VoIP Gateway> (Brug VoIP-gateway) i <VoIP Gateway Settings> (Indstillinger for VoIP-gateway) er alle indstillet til <Off> (Fra) Det er ikke muligt at bruge IP-fax
Begræns mDNS-port	Portnummer 5353 I <mDNS Settings> (mDNS-indstillinger) er indstillingerne <Use IPv4 mDNS> (Brug IPv4 mDNS) og <Use IPv6 mDNS> (Brug IPv6 mDNS) indstillet til <Off> (Fra) <Use Mopria> (Brug Mopria) er indstillet til <Off> (Fra) Det er ikke muligt at søge på netværket eller udføre automatiske indstillinger ved hjælp af mDNS. Det er heller ikke muligt at printe med Mopria™ eller AirPrint
Begræns SLP-port	Portnummer 427 I <Multicast Discovery Settings> (Indstillinger for Multicast-registrering) er <Response> (Svar) indstillet til <Off> (Fra) Det er ikke muligt at søge på netværket eller udføre automatiske indstillinger ved hjælp af SLP
Begræns SNMP-port	Portnummer 161 Du kan muligvis ikke hente eller indstille enhedsoplysningerne fra printerdriveren eller administrationssoftwaren, hvis SNMP-porten er begrænset I <SNMP Settings> (SNMP-indstillinger) er indstillingerne <Use SNMPv1> (Brug SNMPv1) og <Use SNMPv3> (Brug SNMPv3) indstillet til <Off> (Fra)

2. Godkendelse	Bemærkninger
Driftspolitik for godkendelse	
Forbyd gæstebrugere	• <Advanced Space Settings> (Indstillinger for Advanced Space) > <Authentication Management> (Godkendelsesstyring) er indstillet til <On> (Til) • <Login Screen Display Settings> (Skærmindstillinger for loginskærm) er indstillet til <Display When Device Operation Starts> (Vis, når betjening af enhed starter) • <Restrict Job from Remote Device without User Auth> (Begræns job fra fjernenhed uden brugergodk.) er indstillet til <On> (Til) Det er ikke muligt for uregistrerede brugere at logge på maskinen. Printjob sendt fra en computer annulleres også
Gennemtving indstilling af automatisk logout	Denne indstilling er til at logge af kontrolpanelet. Dette gælder ikke for andre metoder til at logge af (kan indstilles i intervaller fra 10 sekunder - 9 minutter) <Auto Reset Time> (Tid for automatisk nulstilling) er aktiveret. Brugeren logges automatisk af, hvis der ikke udføres nogen handlinger i et angivet tidsrum Vælg [Time until Logout] (Tid til logout) på indstillingsskærmen for fjernbrugerinterfacet
Driftspolitik for adgangskode	
Forbyd cachelagring af adgangskode for eksterne servere	Denne indstilling gælder ikke for adgangskoder, som brugeren udtrykkeligt gemmer, f.eks. adgangskoder til adressebøger osv. <Prohibit Caching of Authentication Password> (Forbyd cachelagring af godkendelsesadgangskode) er indstillet til <On> (Til) Brugere skal altid indtaste en adgangskode, når de tilgår en ekstern server
Vis advarsel, når standardadgangskoden er i brug	<Display Warning When Default Password Is in Use> (Vis advarsel, når standardadgangskoden er i brug) er indstillet til <On> (Til) Der vises en advarsel, hver gang maskinens standardadgangskode anvendes
Forbyd brug af standardadgangskode til fjernadgang	<Allow Use of Default Password for Remote Access> (Tillad brug af standardadgangskode til fjernadgang) er indstillet til <Off> (Fra) Det er ikke muligt at bruge fabriksstandardadgangskoden, når maskinen tilgås fra en computer
Politik for adgangskodeindstillinger (politikken gælder ikke for administration af Afdelings-ID eller pinkode)	
Angiv det mindste antal tegn for adgangskoden	Det mindste antal tegn kan indstilles mellem 1 og 32
Angiv gyldighedsperioden for adgangskoden	Gyldighedsperioden kan indstilles mellem 1 og 180 dage
Forbyd brug af 3 eller flere identiske fortløbende tegn	
Gennemtving brug af mindst 1 stort bogstav	
Gennemtving brug af mindst 1 lille bogstav	
Gennemtving brug af mindst 1 ciffer	
Gennemtving brug af mindst 1 symbol	
Politik for spærring	
Aktivér spærring	Gælder ikke for Afdelings-ID/pinkode til mailboks, pinkode eller godkendelse for Sikkert print osv. Spærringsgrænse: Kan indstilles til mellem 1–10 gange Spærringsperiode: Kan indstilles til mellem 1–60 minutter

3. Nøgle/certifikat	Bemærkninger
Forbyd brug af svag kryptering	Gælder for IPSec, TLS, Kerberos, S/MIME, SNMPv3 og trådløst LAN Du kan muligvis ikke kommunikere med enheder, der kun understøtter svag kryptering
Forbyd brug af nøgle/certifikat med svag kryptering	Gælder for IPSec, TLS og S/MIME Hvis du bruger en nøgle/et certifikat med svag kryptering til TLS, ændres den/det forudinstallerede nøgle/certifikat. Du vil ikke kunne kommunikere, hvis du bruger en nøgle/et certifikat med svag kryptering til andre funktioner end TLS
Brug TPM til at gemme adgangskode og nøgle	Kun tilgængelig for enheder med TPM installeret. Tag altid en sikkerhedskopi af TPM-nøglerne, når TPM er aktiveret. Se brugervejledningen for at få yderligere oplysninger Vigtigt, når TPM-indstillingerne er aktiveret: • Sørg for at ændre "Administrator"-adgangskoden fra standardindstillingen for at forhindre, at en anden tredjepart end administratoren kan sikkerhedskopiere TPM-nøglen. Hvis en tredjepart tager TPM-sikkerhedskopinøglen, kan du ikke gendanne TPM-nøglen • For at give øget sikkerhed kan TPM-nøglen kun sikkerhedskopieres én gang. Hvis TPM-indstillingerne er aktiveret, skal du sørge for at sikkerhedskopiere TPM-nøglen til en USB-hukommelsesenhed og gemme den et sikkert sted for at forhindre tab eller tyveri • TPM-sikkerhedsfunktionerne garanterer ikke fuldstændig beskyttelse af data og hardware

4. Log	Bemærkninger
Gennemtving registrering af overvågningslog	• <Save Operation Log> (Gem driftslog) er indstillet til <On> (Til) • <Display Job Log> (Vis joblog) er indstillet til <On> (Til) • <Retrieve Job Log with Management Software> (Hent joblog med administrationssoftware) i <Display Job Log> (Vis joblog) er indstillet til <Allow> (Tillad) • <Save Audit Log> (Gem overvågningslog) er indstillet til <On> (Til) • <Retrieve Network Authentication Log> (Hent log for netværksgodkendelse) er indstillet til <On> (Til) Overvågningslogfiler registreres altid, når denne indstilling er aktiveret
Gennemtving SNTP-indstillinger	Indtast SNTP-serveradresse I <SNTP Settings> (SNTP-indstillinger) er <Use SNTP> (Brug SNTP) indstillet til <On> (Til). Tidssynkronisering via SNTP påkrævet. Angiv en værdi for [Server Name] (Servernavn) på indstillingsskærmen for Remote UI (Fjernbrugerinterface)
Syslog-lograpportering	Aktivér oplysninger om Syslog-destination, når du bruger en Syslog-server eller SIEM • <Username and password> (Brugernavn og adgangskode) • <SMB server name> (SMB-servernavn) • <Destination path> (Destinationssti) • <Perform export time> (Udfør eksporttid)

5. Job	Bemærkninger
Printpolitik	
Forbyd øjeblikkeligt print af modtagne job	Modtagne job gemmes i fax-/I-Fax-hukommelsen, hvis øjeblikkeligt print af modtagne job er forbudt • <Handle Files with Forwarding Errors> (Håndtér filer med videresendelsesfejl) er indstillet til <Off> (Fra) • <Use Fax Memory Lock> (Brug faxhukommelseslås) er indstillet til <On> (Til) • <Use I-Fax Memory Lock> (Brug I-Fax-hukommelseslås) er indstillet til <On> (Til) • <Memory Lock End Time> (Sluttidspunkt for hukommelseslås) er indstillet til <Off> (Fra) • <Display Print When Storing from Printer Driver> (Vis print ved lagring fra printerdriver) i <Set/Register Confidential Fax Inboxes> (Indstil/registrér Fortrolig faxboks) er indstillet til <Off> (Fra) • <Settings for All Mail Boxes> (Indstillinger for alle mailbokse) > <Print When Storing from Printer Driver> (Print ved lagring fra printerdriver) er indstillet til <Off> (Fra) • <Box Security Settings> (Bokssikkerhedsindstillinger) > <Display Print when Storing from Printer Driver> (Vis print ved lagring fra printerdriver) er indstillet til <Off> (Fra) • <Prohibit Job from Unknown User> (Forbyd job fra ukendt bruger) er indstillet til <On> (Til), og <Forced Hold> (Tvunget tilbageholdelse) er indstillet til <On> (Til). Print sker ikke med det samme, selv når der udføres printhandlinger
Politik for afsendelse/modtagelse	
Tillad kun afsendelse til registrerede adresser	I <Limit New Destination> (Begræns ny destination) er indstillingerne <Fax>, <E-mail>, <I-Fax> og <File> (Fil) indstillet til <On> (Til) Det er kun muligt at sende til destinationer, der er registreret i adressebogen
Gennemtving bekræftelse af faxnummer	Brugere skal indtaste et faxnummer igen for at bekræfte, når de sender en fax
Forbyd automatisk videresendelse	<Use Forwarding Settings> (Brug indstillinger for videresendelse) er indstillet til <Off> (Fra) Det er ikke muligt at videresende fax automatisk

6. Lagring	Bemærkninger
Gennemtving fuldstændig sletning af data	<Hard Disk Data Complete Deletion> (Fuldstændig sletning af harddiskdata) er indstillet til <On> (Til)

Du kan finde alle imageRUNNER ADVANCE-specifikationer på produktets webside på https://www.canon.dk/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Danmark
Knud Højgaards Vej 1
2860 Søborg
Tlf.: 70 15 50 05
canon.dk

Canon Inc.
canon.com

Canon Europe
canon-europe.com

Danish edition v1.0©
Canon Europa N.V., 2020