SIKKERHETSVEILEDNING FOR MULTIFUNKSJONSENHETER

imageRUNNER ADVANCE

Canon

INNLEDNING

Med moderne Canon multifunksjonsenheter (MFD-er) kan du skrive ut, kopiere, skanne, sende dokumenter og sende fakser. MFD-er fungerer som egne dataservere, med en rekke nettverkstjenester og betydelig lagringsplass på harddisken.

Organisasjoner som introduserer disse enhetene i infrastrukturen, må ta tak i en rekke områder som en del av den bredere sikkerhetsstrategien for å beskytte nettverkssystemenes konfidensialitet, integritet og tilgjengelighet.

Distribueringen vil klart variere, og organisasjoner vil ha sine egne sikkerhetskrav. Mens vi samarbeider for å sikre at Canon-enheter leveres med de riktige sikkerhetsinnstillingene, tar vi sikte på å støtte dette ytterligere med en rekke konfigurasjonsinnstillinger du kan bruke til å tilpasse enheten så den passer bedre til behovene for akkurat deres situasjon.

Dette dokumentet gir deg informasjonen du trenger for å kunne diskutere med Canon eller Canon-partnere om hvilke innstillingene som passer best for ditt miljø. Det er ikke all enhetsmaskinvare som har like stor kapasitet, og ulike systemprogramvarer kan gi forskjellig funksjonalitet. Når dere har bestemt dere, kan den endelige konfigurasjonen brukes i enheten eller enhetene deres. Det er bare å kontakte Canon-representanten deres for mer informasjon støtte.

Hvem er dette dokumentet ment for?

Dette dokumentet er rettet mot alle som er opptatt av design, implementering og sikring av multifunksjonsenheter for kontoret (MFD-er) innenfor en nettverksinfrastruktur. Dette kan omfatte IT- og nettverksspesialister, fagfolk som jobber med IT-sikkerhet og servicepersonell.

Omfang og dekning

Veiledningen forklarer og gir råd om konfigurasjonsinnstillingene for to typiske nettverksmiljøer, slik at organisasjoner kan implementere en MFD-løsning på en sikker måte basert på beste praksis. Den forklarer også (fra versjon 3.8 av systemprogramvaren) hvordan Syslog-funksjonaliteten kan gi tilbakemeldinger i sanntid fra MFD. Disse innstillingene er testet og godkjent av Canons sikkerhetsteam.

Vi gjør ingen antagelser om spesielle bransjemessige forskriftskrav som kan pålegge andre sikkerhetsvurderinger og ikke er inkludert i dette dokumentets omfang.

Denne håndboken ble laget basert på det typiske funksjonssettet til imageRUNNER ADVANCE-plattformen. Selv om informasjonen i håndboken gjelder for alle modeller og serier i imageRUNNER ADVANCE-serien, kan noen funksjoner variere mellom modeller.

Implementere riktig MFD-sikkerhet for miljøet deres

Vi har vurdert to typiske scenarioer for å utforske hva det å implementere en flerfunksjonsenhet som en del av nettverket vil ha å si for sikkerheten:

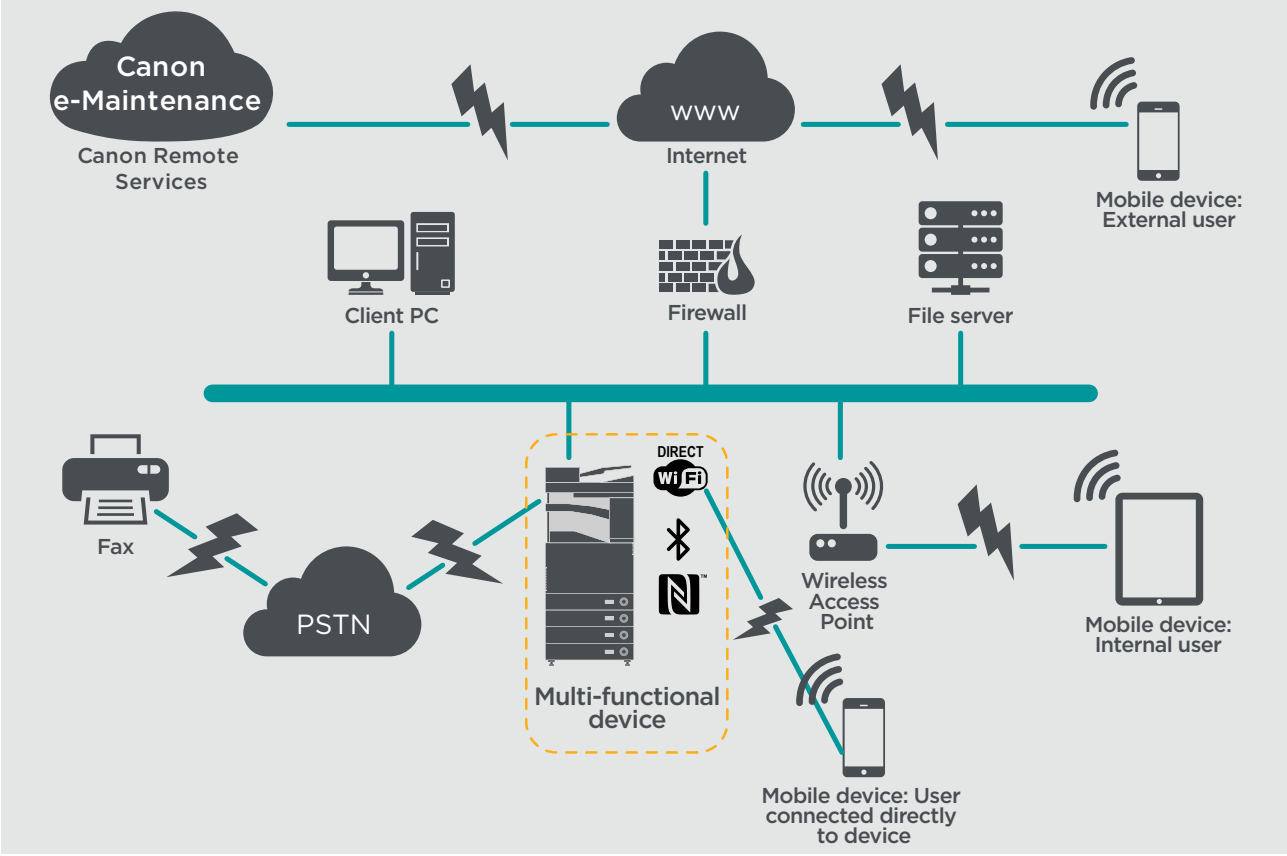
- **Et typisk lite kontormiljø**
- **Et typisk kontormiljø i en bedrift**

LITE KONTORMILJØ

Dette vil vanligvis være et småbedriftsmiljø med en ikke segmentert nettverkstopologi. Det bruker én eller to MFD-er for intern bruk, og disse enhetene er ikke tilgjengelige på Internett.

Mobilutskrift er tilgjengelig, men krever flere løsningskomponenter. Brukere som trenger utskriftstjenester utenfor et LAN-miljø, må ha en sikker tilkobling, men dette dekkes ikke i denne veiledningen. Du bør imidlertid være oppmerksom på sikkerheten til dataene som overføres mellom den eksterne enheten og utskriftsinfrastrukturen.

Figur 1 Nettverk for små kontorer



Siste generasjons imageRUNNER ADVANCE-modeller har trådløs nettverkstilkobling som gjør at enheten kan kobles til et trådløst nettverk. De kan også brukes til å opprette en WiFi Direct-tilkobling fra punkt til punkt med en mobil enhet, uten behov for en nettverkstilkobling.

Alternativer for Bluetooth og NFC er tilgjengelige for flere enhetsmodeller og brukes bare til å opprette WiFi Direct-tilkoblingen for henholdsvis iOS- og Android-enheter.

KONFIGURERINGSHENSYN

Vær oppmerksom på at med mindre en funksjon i imageRUNNER ADVANCE er nevnt nedenfor, anses det som tilstrekkelig i standardinnstillingene for dette bedrifts- og nettverksmiljøet.

Tabell 1 Konfigureringshensyn for små kontormiljøer

imageRUNNER ADVANCE-funksjon	Beskrivelse	Hensyn
Servicemodus	Gir tilgang til innstillinger for servicemodus	Beskytt med et passord som ikke er standard, ikke er vanlig og har maksimal lengde
System for tjenestebehandling	Gir tilgang til ulike enhetsinnstillinger som ikke er standard	Beskytt med et passord som ikke er standard, ikke er vanlig og har maksimal lengde
SMB – Bla gjennom/send	Lagre til og hent fra delte Windows-/SMB-nettverksressurser	Systemadministratorer bør sette opp policyer som forbyr at brukere oppretter lokale kontoer på klientmaskinen for å dele dokumenter med imageRUNNER ADVANCE over SMB
Eksternt brukergrensesnitt	Nettbasert konfigurasjonsverktøy	imageRUNNER ADVANCE-administratoren bør aktivere HTTPS for det eksterne brukergrensesnittet og deaktivere HTTP-tilgang. Aktiver autentisering med PIN-kode som er unik for hver enhet
SNMP	Integrering av nettverksovervåking	Deaktiver versjon 1 og aktiver kun versjon 3
Send til e-post og/eller IFAX	Send e-postmeldinger med vedlegg fra enheten	Aktiver SSL Ikke bruk POP3-autentisering før SMTP-sending Bruk SMTP-autentisering
POP3	Hent og skriv ut dokumenter fra postkassen automatisk	Aktiver SSL Aktiver POP3-autentisering
Adressebok/LDAP	Bruk katalogtjenesten til å slå opp telefonnumre eller e-postadresser skannede elementer skal sendes til	Aktiver SSL Ikke bruk domenelegitimasjon til autentisering mot LDAP-serveren. Bruk LDAP-spesifikk legitimasjon
FTP-utskrift	Last opp og last ned dokumenter til og fra den innebygde FTP-serveren	Slå på FTP-autentisering. Vær oppmerksom på at FTP-trafikk alltid går i klartekst over nettverket
WebDAV-sending	Skann og lagre dokumenter på en ekstern plassering	Aktiver godkjenning for delte WebDAV-ressurser
Kryptert PDF	Krypter dokumenter	Policyen bør være at sensitive dokumenter krypteres med kun PDF-versjon 1.6 (AES-128)
Sikker utskrift	Utskriftsjobben sendes til enheten, men blir liggende i utskriftskøen frem til man taster inn PIN-koden	Aktiver utskriftsjobber beskyttet med PIN-kode
Varsling om Syslog-hendelse	System Logging Protocol er en standardprotokoll i bransjen, og brukes til å sende systemlogg- eller hendelsesmeldinger til en bestemt server kalt en Syslog-server	Vurder å peke Syslog-dataene for imageRUNNER til det eksisterende verktøyet for analysering av nettverkets Syslog eller SIEM-plattformen.
Bekreft systemet ved oppstart	Sikrer at komponentene i systemprogramvaren ikke er kompromittert. Dette har minimal påvirkning på systemets oppstartstid	Aktiver funksjon
Innebygd nettleser	Nettlesertilgang til Internett	Håndheve med administrasjon, bruk av en innholdsfiltrerende webproxy for å unngå at skadelig innhold eller innhold med virus åpnes. Deaktiver oppretting av favoritter
Bluetooth og NFC (tilgjengelig fra Generation 3-modeller)	Brukes til å opprette en WiFi Direct-tilkobling	Aktiver WiFi Direct for å tillate direkte tilkobling til en mobilenhet. WiFi Direct kan ikke brukes når WiFi brukes til å koble til et nettverk
Trådløst LAN	Gir trådløs tilgang	Bruk WPA-PSK/WPA2-PSK med sterke passord
IPP	Koble til og send utskriftsjobber via IP	Deaktiver IPP

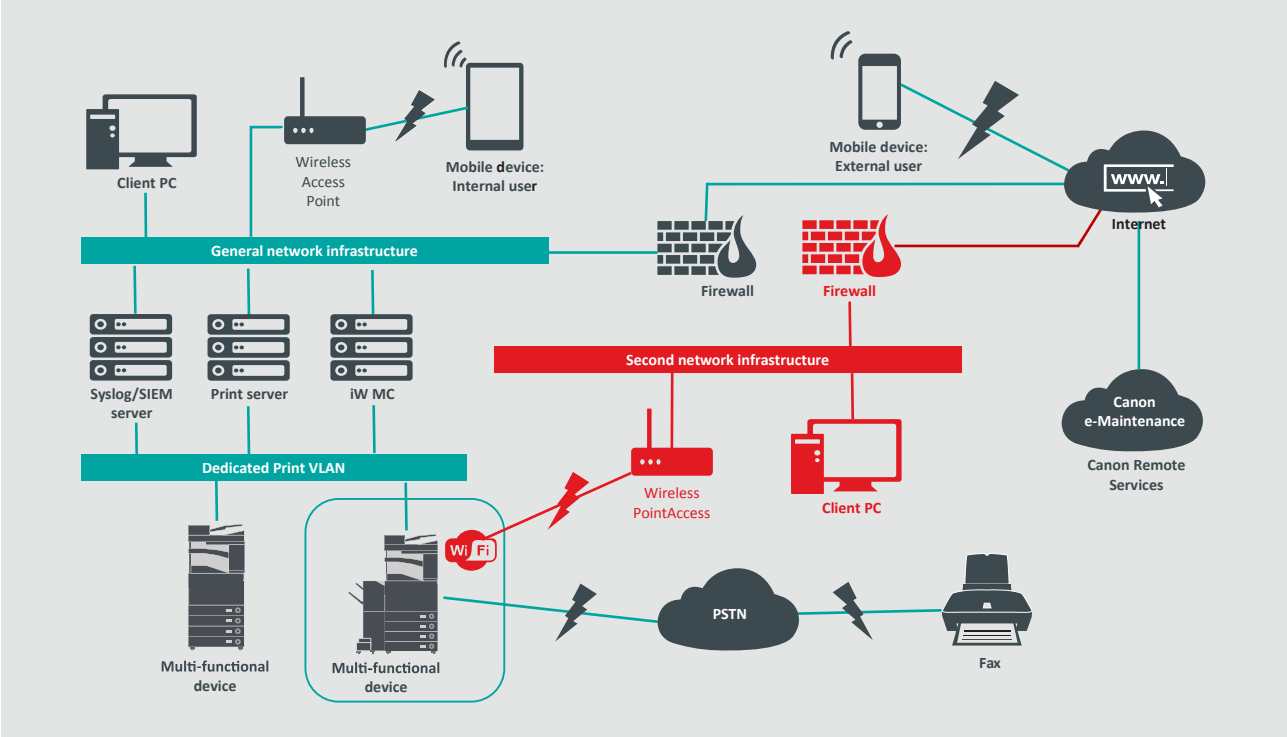
ET KONTORMILJØ I EN BEDRIFT

Dette er vanligvis et miljø med flere steder og kontorer med segmentert nettverksarkitektur. Det har flere MFD-er fordelt på et eget VLAN-nettverk som er tilgjengelig for intern bruk via en eller flere utskriftsservere. Disse MFD-ene er ikke tilgjengelige fra Internett.

Dette miljøet vil vanligvis ha et permanent team for å dekke nettverks- og back office-behovene, i tillegg til generelle dataproblemer, men det antas at de ikke vil ha spesifikk opplæring i MFD.

Dette er vanligvis et miljø med flere steder og kontorer med segmentert nettverksarkitektur. Det har flere MFD-er fordelt på et eget VLAN-nettverk som er tilgjengelig for intern bruk via en eller flere utskriftsservere. Disse MFD-ene er ikke tilgjengelige fra Internett.

Figur 2 Kontorarbeid i større bedrifter



Tilkoblinger uthevet i rødt er tilgjengelig fra og med Generation 3-modellene

KONFIGURERINGSHENSYN

Vær oppmerksom på at med mindre en funksjon i imageRUNNER ADVANCE er nevnt nedenfor, anses det som tilstrekkelig i standardinnstillingene for dette bedrifts- og nettverksmiljøet.

Tabell 2 Konfigureringshensyn for kontormiljøer i større bedrifter

imageRUNNER ADVANCE-funksjon	Beskrivelse	Hensyn
Servicemodus	Gir tilgang til innstillinger for servicemodus	Beskytt med et passord som ikke er standard, ikke er vanlig og har maksimal lengde
System for tjenestebehandling	Gir tilgang til forskjellige ikke-standard enhetsinnstillinger	Beskytt med et passord som ikke er standard, ikke er vanlig og har maksimal lengde
SMB – Bla gjennom/send	Lagre til og hent fra delte Windows-/SMB-nettverksressurser	Systemadministratorer bør sette opp policyer som forbyr at brukere oppretter lokale kontoer på maskinen for å dele dokumenter med imageRUNNER ADVANCE over SMB
Eksternt brukergrensesnitt	Nettbasert konfigurasjonsverktøy	Etter innledende enhetskonfigurasjoner deaktiverer du det eksterne brukergrensesnittet helt ved å deaktivere HTTP og HTTPS
SNMP	Integrering av nettverksovervåking	Deaktiver versjon 1 og aktiver kun versjon 3
Send til e-post og/eller IFAX	Send e-postmeldinger med vedlegg fra enheten	Aktiver SSL Aktiver følgende: - Sertifikatbekreftelse på SMTP-serveren Eller, hvis dette ikke er mulig: - Bruk denne funksjonen kun i et miljø der det finnes en Network Intruder Detection System-innsamler. Ikke bruk POP3-autentisering før SMTP-sending med SMTP-autentisering
POP3	Hent og skriv ut dokumenter fra postkassen automatisk	Aktiver SSL Aktiver følgende: - Sertifikatbekreftelse på POP3-serveren Eller, hvis dette ikke er mulig: - Bruk denne funksjonen kun i et miljø der det finnes en Network Intruder Detection System-innsamler. Aktiver POP3-autentisering
Adressebok/LDAP	Bruk katalogtjenesten til å slå opp telefonnumre eller e-postadresser skannede elementer skal sendes til	Aktiver SSL Aktiver følgende: - Sertifikatbekreftelse på LDAP-serveren Eller, hvis dette ikke er mulig: - Bruk denne funksjonen kun i et miljø der det finnes en Network Intruder Detection System-innsamler. Ikke bruk domenelegitimasjon til autentisering mot LDAP-serveren. Bruk LDAP-spesifikk legitimasjon
IPP	Koble til og send utskriftsjobber via IP	Deaktiver IPP
WebDAV-sending	Skann og lagre dokumenter på en ekstern plassering	Aktiver godkjenning for delte WebDAV-ressurser. Aktiver SSL Tving skriveren til å tillate opplasting av kun filer med filtyper for filutskrift
IEEE802.1X	Godkjenningsmekanisme for nettverkstilgang	Support EAPOL V1
Kryptert PDF	Krypter dokumenter	Policyen bør være at sensitive dokumenter krypteres med kun PDF-versjon 1.6 (AES-128)
Kryptert sikker utskrift	Forbedre beskyttelsen av sikker utskrift ved å kryptere filen og passordet under overføringen	Konfigurer brukernavnet i fanen Skriver i klientens skriverkonfigurasjon til et annet brukernavn enn brukerens LDAP/domenelegitimasjon. Sørg for at Begrens utskriftsjobber er slått av
Automatisk registrering av sertifikat	Den automatiske registreringsprosessen forbedrer effektiviteten ved innhenting og distribusjon av digitale sertifikater	Krever en nettverkssertifikatløsning for å bruke
Varsling om Syslog-hendelse	System Logging Protocol er en standardprotokoll i bransjen, og brukes til å sende systemlogg- eller hendelsesmeldinger til en bestemt server kalt en Syslog-server	Vurder å peke Syslog-dataene for imageRUNNER ADVANCE til det eksisterende verktøyet for analysering av nettverkets Syslog eller SIEM-plattformen
Bekreft systemet ved oppstart	Sikrer at komponentene i systemprogramvaren ikke er kompromittert. Dette har minimal påvirkning på systemets oppstartstid	Aktiver funksjon
Trådløst LAN	Gir trådløs tilgang	Bruk WPA-PSK/WPA2-PSK med sterke passord
WiFi Direct	Brukes til å opprette en WiFi Direct-tilkobling	Deaktiver WiFi Direct
Innebygd nettleser (tilgjengelig fra 2. utgave av Generation 3-modeller)	Nettlesertilgang til Internett	Bruk tilstrekkelige begrensninger eller deaktiver muligheten til å laste ned filer som er hentet fra nettleseren

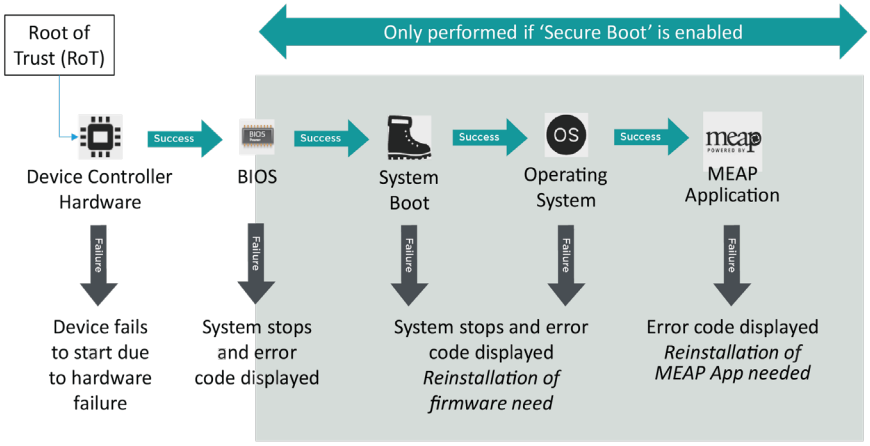
Siste generasjons imageRUNNER ADVANCE-modeller har trådløs nettverkstilkobling som gjør at enheten kan kobles til et trådløst nettverk samtidig som de er koblet til et kablet nettverk. Dette scenarioet kan være nyttig når kunden må dele en enhet over to nettverk. Et skolemiljø er et typisk eksempel der man har separate nettverk for ansatte og elever.

imageRUNNER ADVANCE-plattformen gir et funksjonsmiljø med fleksibel bruk. Når protokoller og tjenester er tilgjengelige for å oppnå dette, er det viktig å sikre at kun de nødvendige funksjonene, tjenestene og protokollene er aktivert for å oppfylle brukerens behov. Dette er god sikkerhetspraksis, og vil redusere den potensielle angrepsoverflaten og hindre at de utnyttes. Det dukker stadig opp nye sikkerhetsproblemer. Derfor må vi alltid være på vakt for trusler, enten de kommer utenfra eller er iboende i enheten. Muligheten til å overvåke brukeraktivitet hjelper oss med å identifisere og iverksette tiltak når det trengs.

Versjon 3.8 av programvareplattformen for imageRUNNER ADVANCE inneholder ekstra funksjoner i tillegg til de den har hatt i flere år. Dette inkluderer muligheten til å overvåke enheten i sanntid ved hjelp av Syslog og Bekreft systemet ved oppstart. Med disse funksjonene og de eksisterende nettverkssikkerhetsløsningene, for eksempel en Security Information Event Management-plattform eller en loggføringsløsning, får du bedre oversikt og kan identifisere og håndtere hendelser som oppstår.

Bekreft systemet ved oppstart

Denne funksjonaliteten er en maskinvaremekanisme som er utformet for å sikre at alle deler av systemprogramvaren for 3. utgave av imageRUNNER ADVANCE Generation 3 verifiseres mot en Root of Trust for å sikre at operativsystemet lastes inn slik Canon har tiltenkt. Hvis uvedkommende skulle tukle med eller prøve å endre systemet, eller hvis det skulle oppstå en feil under lasting av systemet, stoppes prosessen og en feilkode vises.



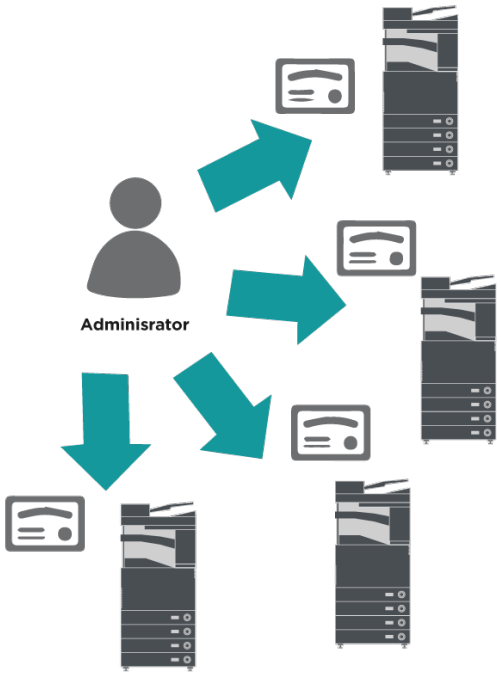
Figur 3 Prosess for Bekreft systemet ved oppstart

Denne prosessen er transparent for brukeren, bortsett fra skjermen som indikerer at en utilsiktet systemversjon er lastet inn. I 3. utgave av imageRUNNER ADVANCE Generation er det et alternativ for å aktivere Bekreft systemet ved oppstart, som må slås på for å aktivere denne sikkerhetsfunksjonen.

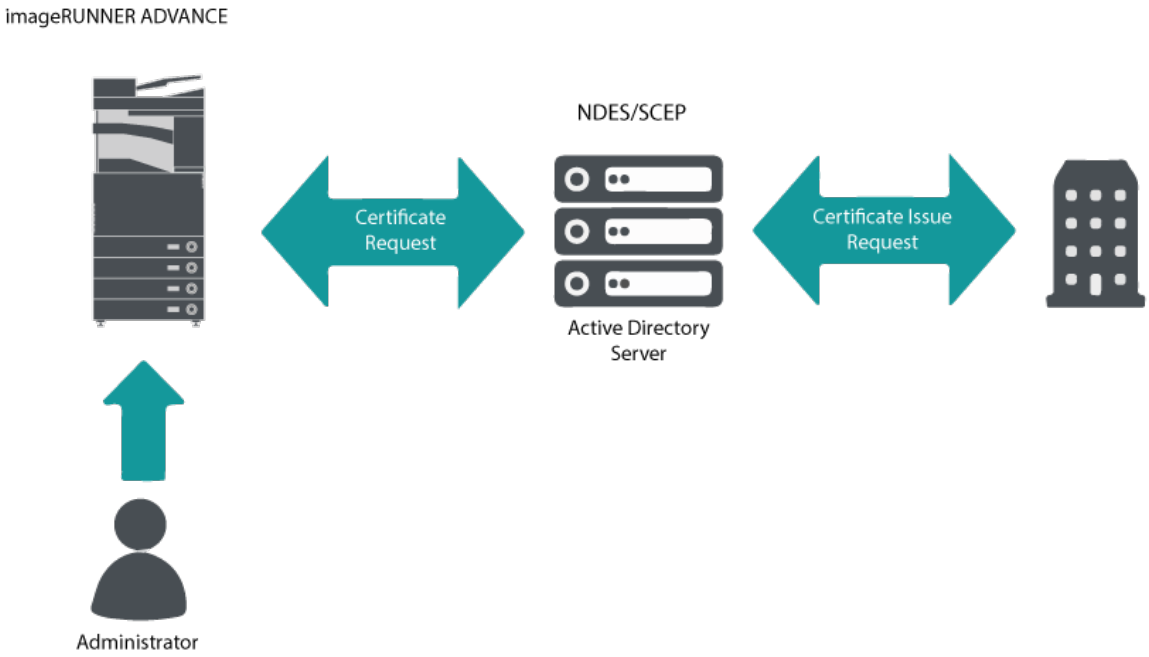
Automatisk registrering av sertifikat

Før versjon 3.8 av plattformversjoner av imageRUNNER ADVANCE-systemprogramvaren måtte administratoren installere oppdaterte sikkerhetssertifikater manuelt på hver enhet. Dette er en arbeidskrevende oppgave, da man må koble til hver enhet for å kjøre en manuell oppdatering. Sertifikater må installeres manuelt ved hjelp av den bestemte enhetens eksterne brukergrensesnitt (RUI), noe som gjør prosessen mye mer tidkrevende. Tjenesten Automatisk registrering av sertifikat ble innført fra plattformversjon 3.8 og senere, og eliminerer dette ekstraarbeidet.

Den automatiske registreringsprosessen forbedrer effektiviteten ved innhenting av sertifikater. Med denne prosessen kan sertifikater hentes automatisk ved hjelp av Network Device Enrolment Service (NDES) for Microsoft Windows og Simple Certificate Enrolment Protocol (SCEP).



Figur 4 Registrering av sertifikat



Figur 5 Prosess for registrering av sertifikat

SCEP er en protokoll som støtter sertifikater utstedt av en sertifiseringsinstans, og NDES gjør at nettverksenheter kan hente eller oppdatere sertifikater basert på SCEP.

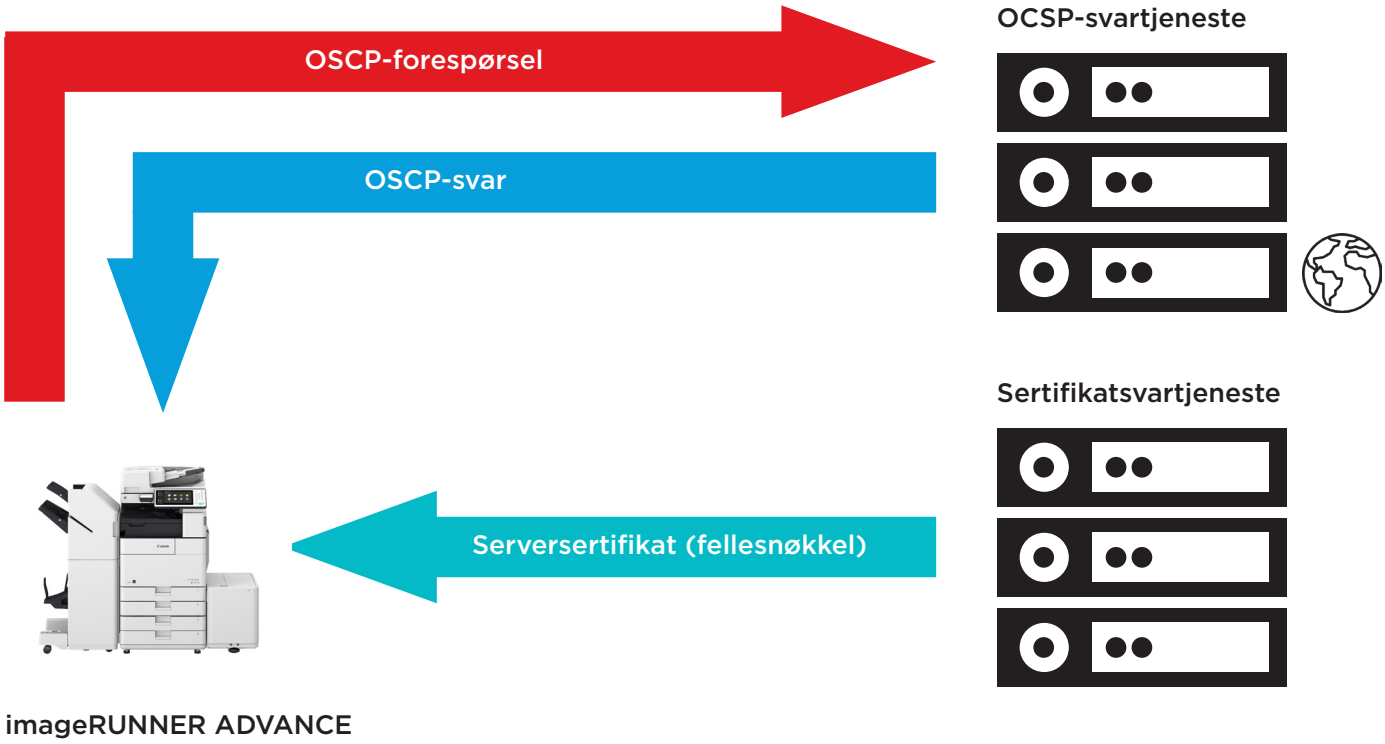
NDES er en rolletjeneste for Active Directory-sertifikattjenester.

Online Certificate Status Protocol

Det er mange grunner til at det kan være nødvendig å trekke tilbake et digitalt sertifikat. Det kan for eksempel hende at den private nøkkelen er mistet, stjålet eller skadet, eller at et domenenavn er endret.

OCSP (Online Certificate Status Protocol) er en standard Internett-protokoll som brukes til å sjekke opphevelsesstatusen til et digitalt X.509-sertifikat som ble gitt av sertifikatserveren. Når man sender en OCSP-forespørsel om et bestemt sertifikat til OCSP-svartjenesten (vanligvis en sertifikatutsteder), svarer OCSP-svartjenesten med «bra», «opphevet» eller «ukjent».

Figur 6 Prosess for OCSP-håndtrykk



Med imageRUNNER ADVANCE fra plattformversjon 3.10 gir OCSP en sanntidsmekanisme for å kontrollere de installerte digitale X.509-sertifikatene. Tidligere plattformversjoner støttet kun CRL-metoder (Certificate Revoke List) som er ineffektive og fører til store kostnader for nettverksressurser.

Administrasjon av sikkerhetsinformasjon og -hendelser

imageRUNNER ADVANCE-teknologien støtter muligheten til å sende ut sikkerhetshendelser i sanntid ved hjelp av Syslog-protokollen som følger RFC 5424, RFC 5425 og RFC 5426.

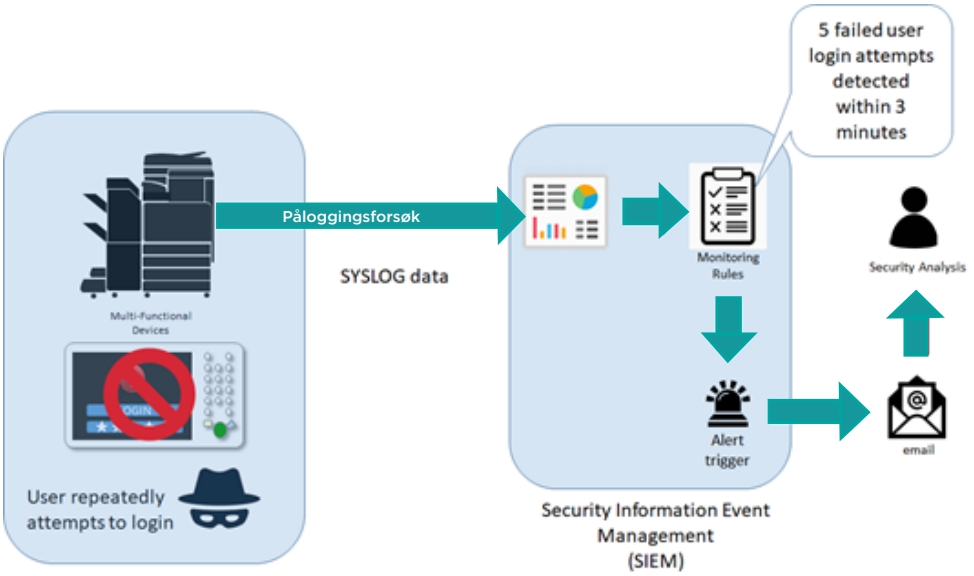
En rekke typer enheter bruker denne protokollen som en metode for å samle inn sanntidsinformasjon som kan brukes til å identifisere potensielle sikkerhetsproblemer.

For å gjøre det enklere å oppdage trusler og sikkerhetshendelser må enheten konfigureres slik at den peker til en SIEM-server (Security Incident Event Management) fra en tredjepart.

Syslog-hendelsene enheten produserer, kan brukes til å opprette handlinger ved hjelp av sanntidsinnsamling og analyse av hendelser fra en rekke kontekstuelle datakilder (figur 7). Den kan også støtte samsvarsrapportering og gransking av hendelser ved hjelp av tilleggsløsninger, for eksempel en SIEM-server. Dette ser man et eksempel på i figur 8.

Siste generasjons imageRUNNER ADVANCE-enheter har Syslog-funksjonalitet som støtter en rekke hendelser som kan samles inn. Dette kan brukes til å korrelere og analysere hendelser fra flere ulike kilder for å identifisere trender eller avvik.

Figur 7 Henting av Syslog-data



Figur 8 Eksempel på bruk av Syslog-data i imageRUNNER ADVANCE

Behandling av enhetslogg

I tillegg til Syslog-funksjonaliteten fra versjon 3.8 av systemprogramvaren har imageRUNNER ADVANCE følgende logger som kan behandles på enheten. Disse loggene kan eksporteres i CSV-filformat med det eksterne brukergrensesnittet (RUI).

Tabell 3 – Eksempler på loggfiler som kan behandles av multifunksjonsenheten.

Type logg	Tall angitt som «Loggtype» i CSV-filen	Beskrivelse
Logg	4098	Denne loggen inneholder informasjon om autentiseringsstatusen for brukerautentisering (pålogging/avlogging og brukerautentisering vellykket/mislykket), registrering/endring/sletting av brukerinformasjon som behandles med Brukerautentisering og behandling (legge til / redigere/slette) av roller med TILGANGSBEHANDLINGSSYSTEMET
Jobblogg	1001	Denne loggen inneholder informasjon om fullføring av kopierings-/faks-/skanne-/sende-/utskriftsjobber
Overføringslogg	8193	Loggen inneholder informasjon om overføringer
Lagringslogg for Advanced Space	8196	Denne loggen inneholder informasjon om lagring av filer på Advanced Space, nettverket (Advanced Space på andre maskiner) og minnemedier
Operasjonslogg for postboksen	8197	Denne loggen inneholder informasjon om operasjonene som utføres på data i postboksen, RX-minneinnboksen og den konfidensielle faksinnboksen
Autentiseringslogg for postboksen	8199	Denne loggen inneholder informasjon om godkjenningsstatusen for postboksen, RX-minneinnboksen og den konfidensielle faksinnboksen
Operasjonslogg for Advanced Space	8201	Denne loggen inneholder informasjon om dataoperasjoner i Advanced Space
Administrasjonslogg for maskinen	8198	Denne loggen inneholder informasjon om oppstart/avslutning av maskinen, endringer i innstillingene ved hjelp av (Innstillinger/Registrering), endringer i innstillingene ved hjelp av funksjonen Device Information Delivery (Levering av enhetsinformasjon) og tidsinnstillingen. Maskinens administrasjonslogg registrerer også endringer i brukerinformasjonen eller sikkerhetsrelaterte innstillinger når maskinen inspiseres eller repareres av den lokale, autoriserte Canon-forhandleren
Autentiseringslogg for nettverket	8200	Denne loggen registreres når IPSec-kommunikasjon mislykkes
Eksporter/importer alle-logg	8202	Denne loggen inneholder informasjon om import/eksport av innstillingene ved hjelp av funksjonen Eksporter alle / importer alle
Sikkerhetskopieringslogg for postboksen	8203	Denne loggen inneholder informasjon om sikkerhetskopiering av data i brukerinnboksene, RX-minneinnboksen, den konfidensielle faksinnboksen og Advanced Space, i tillegg til eventuelle data som er lagret, og skjemaet som er registrert for funksjonen for innkopiering av bilder
Operasjonslogg for skjermbildet for program-/programvareadministrasjon	3101	Dette er en operasjonslogg for SMS (Service Management Service), registrering/oppdateringer av programvare og installasjonsprogrammer for MEAP-programmer osv.
Sikkerhetspolicylogg	8204	Denne loggen inneholder informasjon om innstillingsstatusen til sikkerhetspolicyens innstillinger
Gruppestyringslogg	8205	Denne loggen inneholder informasjon om innstillingsstatusen (registrering/redigering/sletting) til brukergruppene
Systemvedlikeholdslogg	8206	Denne loggen inneholder informasjon om fastvareoppdateringer og sikkerhetskopiering/gjenoppretting av MEAP-programmet osv.
Autentiseringslogg for utskrifter	8207	Denne loggen inneholder informasjon og operasjonshistorikken om utskriftsjobber med tvungen holding
Logg for synkronisering av innstillinger	8208	Denne loggen inneholder informasjon om synkronisering av maskininnstillingene. Synkronisere innstillinger for flere Canon multifunksjonsskrivere
Logg for Administrasjon av logg for sporing av endringer	3001	Denne loggen inneholder informasjon om start og avslutting av denne funksjonen (funksjonen Administrasjon av logg for sporing av endringer) samt eksport av logger osv.

Logger kan inneholde opptil 40 000 oppføringer. Når antallet oppføringer går over 40 000, slettes de eldste oppføringene først.

STØTTE FOR EKSTERNE ENHETER

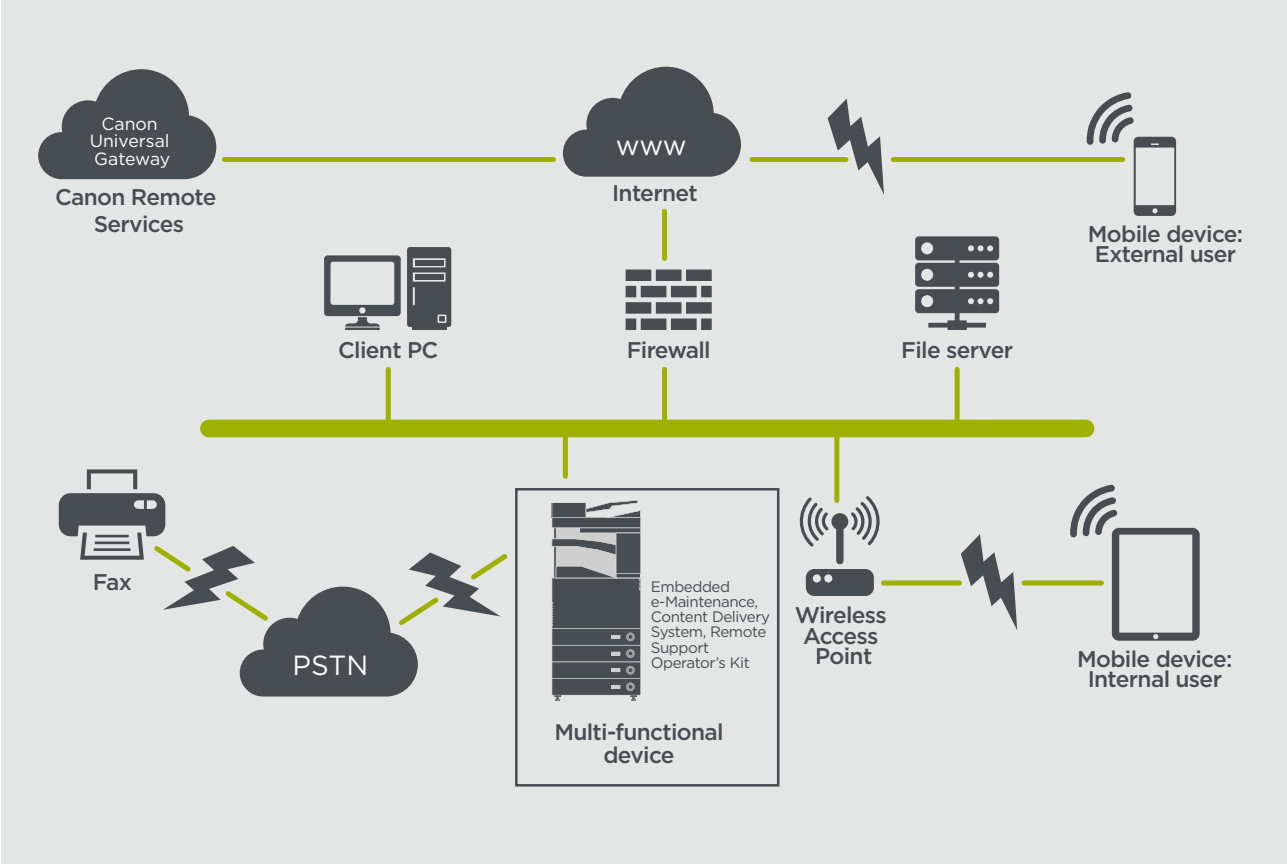
For at Canon eller en Canon-partner skal kunne gi effektiv service, kan imageRUNNER ADVANCE sende tjenesterelaterte data og motta fastvareoppdateringer eller programmer. Vær oppmerksom på at det ikke sendes bildedata eller metadata for bilder.

Nedenfor vises to mulige implementeringer av Canons eksterne tjenester i et bedriftsnettverk.

Implementeringsscenario 1: Spredt tilkobling

I dette scenarioet kan hver MFD kobles direkte til den eksterne tjenesten via Internett.

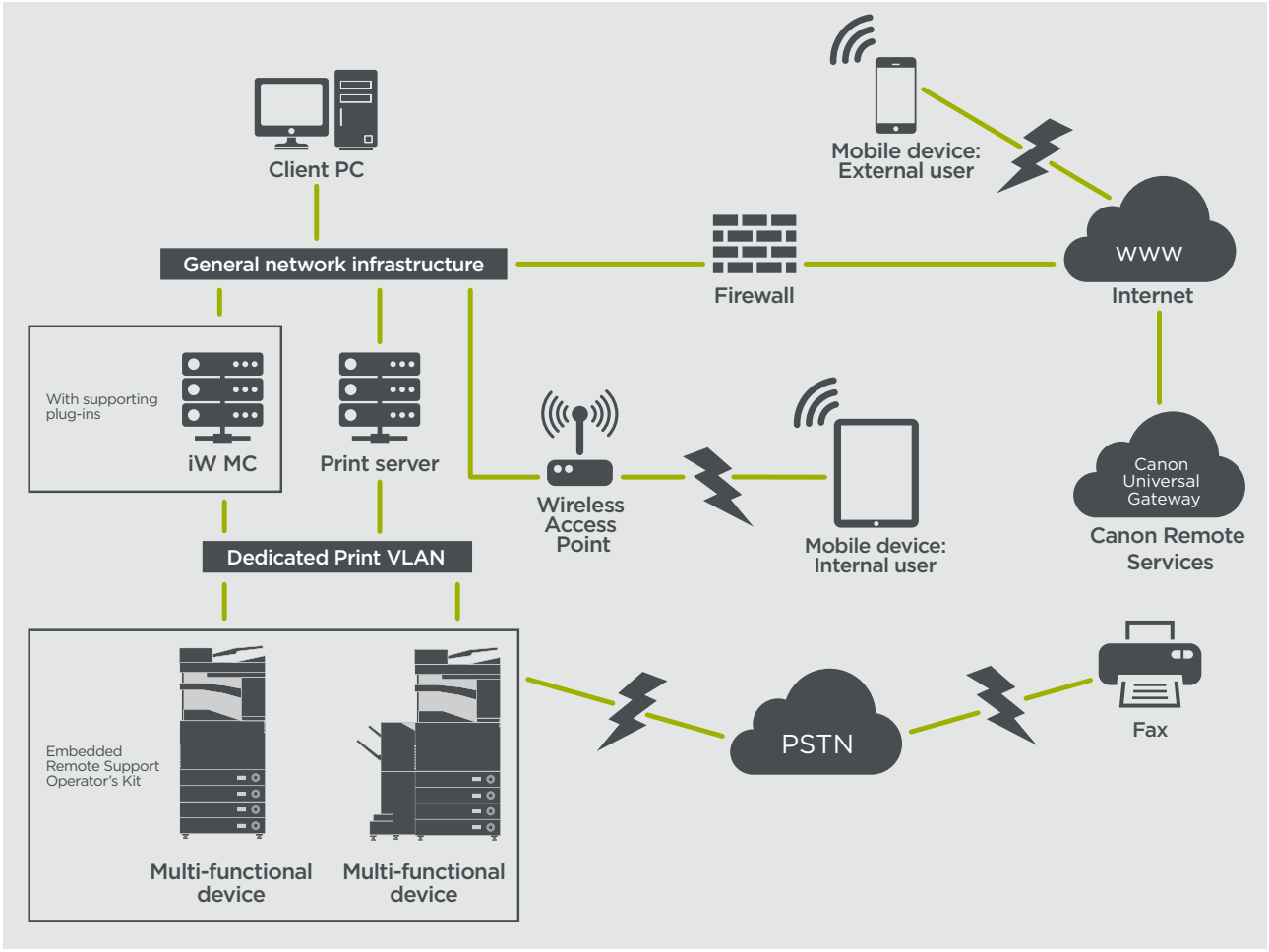
Figur 9 Spredt tilkobling



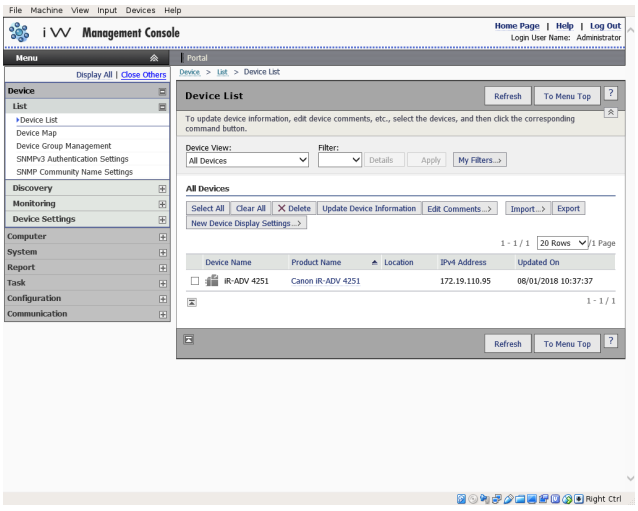
Implementeringsscenario 2: Sentralisert administrert tilkobling

I et scenario for bedriftsmiljøer der flere MFD-er er installert, må man kunne administrere disse enhetene effektivt fra ett sentralt punkt, inkludert tilkobling til Canons eksterne tjenester. For å forenkle den helhetlige tilnærmingen til administrasjon oppretter individuelle enheter administrasjonstilkoblinger via et enkelt iWMC-tilkoblingspunkt (iW Management Console). UDP-port 47545 brukes til kommunikasjon mellom plugin-modulen Device Firmware Upgrade (DFU) og multifunksjonsenheter.

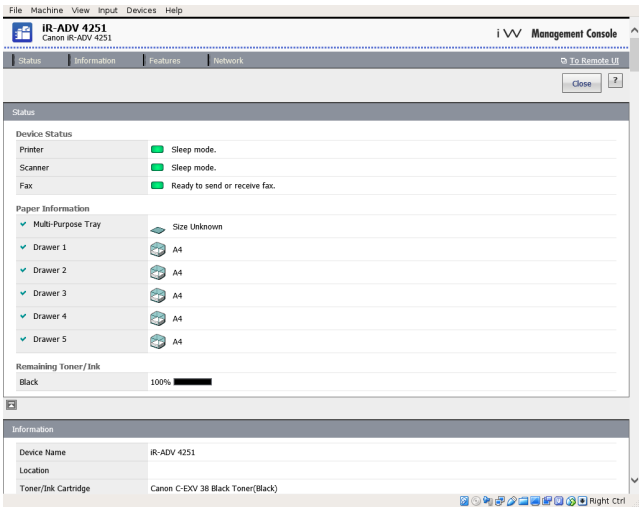
Figur 10 Sentralisert administrert tilkobling



Figur
11a. Enhetsliste (i dette tilfellet en enkelt enhet) som rapportert på imageWARE Management Console og
11b. Enhetsdetaljer og -innstillinger



Figur 11a



Figur 11b

e-Maintenance

e-Maintenance-systemet kan samle inn enhetens brukstellere for faktureringsformål, administrasjon av forbruksvarer og overvåking av eksterne enheter ved hjelp av status- og feilvarslinger.

e-Maintenance-systemet består av en UGW (Internett-rettet server) og enten en innebygd programvare for multifunksjonsenheter (eRDS) og/eller ekstra serverbasert programvare (RDS-plugin) for å hente inn informasjon om service av enheter. ERDS er et overvåkingsprogram som kjøres i imageRUNNER ADVANCE. Hvis overvåkingsalternativet er aktivert i enhetsinnstillingene, innhenter eRDS-systemet sin egen enhetsinformasjon og sender den til UGW. RDS-plugin-modulen er et overvåkingsprogram som installeres på en vanlig datamaskin og kan overvåke mellom 1 og 3000 enheter. Den henter informasjon fra hver enhet via nettverket, og sender den til UGW.

Som vist i tabell 4 nedenfor viser den neste siden dataene som overføres, protokoller (avhengig av hvilke alternativer som er valgt under utformingen og implementeringen) og hvilke porter som brukes. Ingen kopi-, utskrifts-, skanne- eller faksdata overføres.

Tabell 4 Oversikt over e-Maintenance-data

Beskrivelse	Behandlede data	Protokoll/port	Port
Kommunikasjon mellom eMaintenance (plugin-modul eRDS eller RDS) og UGW	Webtjenesteadresse for UGW Proxy-serveradresse / portnummer / proxy-konto / passord Måladresse for UGW-post SMTP-serveradresse POP-serveradresse Enhetsstatus-, teller- og modellinformasjon Serienummer Informasjon om gjenværende toner/ blekk Fastvareinformasjon Informasjon om reparasjonsforespørsel Logginformasjon Servicebesøk Servicealarm Papirstopp Miljø Tilstandslogg	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Kommunikasjon mellom eMaintenance og enheten (bare med RDS-plugin, da eRDS er innebygd programvare)		SNMP Canons proprietære SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Innholdsleveringssystem

Innholdsleveringssystemet (CDS) oppretter en forbindelse mellom MFD og Canon Universal Gateway (UGW). Det kan brukes til å oppdatere fastvare og programmer på enheter.

Tabell 5 Oversikt over innholdsleveringssystemet

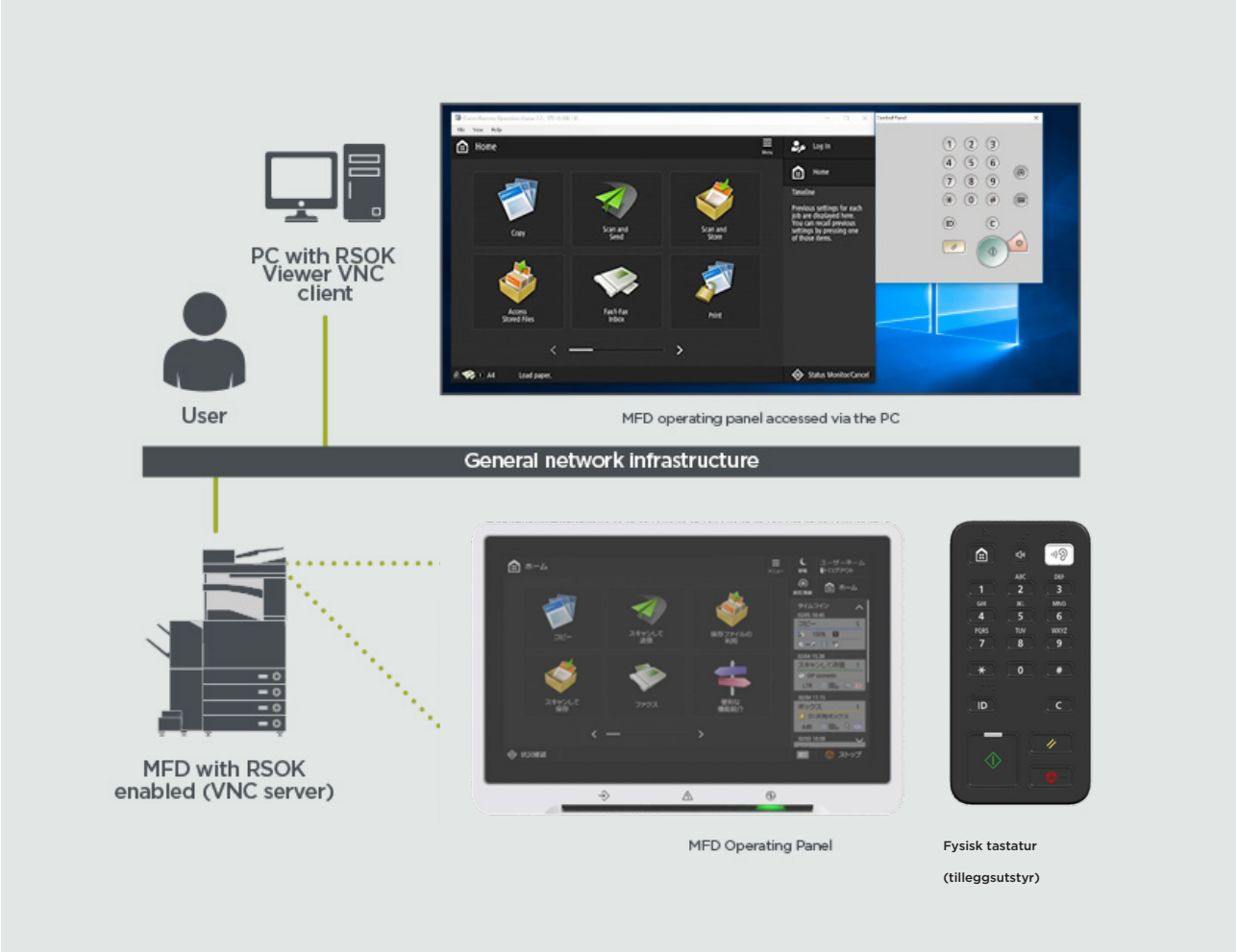
Beskrivelse	Sendte data	Protokoll/port	Port
Kommunikasjon mellom MFD og UGW	Serienummer for enhet Fastvareversjon Språk Land Informasjon lisensavtalen for sluttbrukere av enheten	HTTP/HTTPS	TCP/80 TCP/443
Kommunikasjon mellom UGW og MFD	Testfil (binære tilfeldige data) for kommunikasjonstesting Binære data for fastvare eller MEAP-programmer	HTTP/HTTPS	TCP/80 TCP/443

I enhetskonfigurasjonen er det forhåndsinnstilt en URL-adresse for CDS-tilgang.
Ved behov for sentralisert administrasjon av enhetsfastvare og programmer fra infrastrukturen, installeres det en lokal installasjon av iWMC med plugin-modulen Device Firmware Upgrade (DFU). Man må også ha plugin-modulen Device Application Management for å gjøre dette.

Operatørsett for ekstern støtte

Operatørsettet for ekstern støtte gir ekstern tilgang til enhetens kontrollpanel. Dette serverklientsystemet består av en VNC-server som kjører på MFP og Microsoft Windows-klientprogrammet Remote Operation Viewer VNC.

Figur 12 Konfigurering av operatørsettet for ekstern støtte



Tabell 6 Oversikt over data for operatørsettet for ekstern støtte

Beskrivelse	Sendte data	Protokoll/port	Port
Autentisering av VNC-passord	Brukerpassord	DES-kryptering	5900
Operation Viewer	Enhetens kontrollpanel - skjermbildedata - nøkkeloperasjon for maskinvaren	RFB-protokoll versjon 3.3	5900

VEDLEGG

Sikkerhetsrelaterte funksjoner for Canon imageRUNNER ADVANCE

imageRUNNER ADVANCE-plattformen kan konfigureres eksternt via det eksterne brukergrensesnittet (RUI), et grensesnitt for nettjenester. Dette grensesnittet gir tilgang til mange av enhetens konfigurasjonsinnstillinger og kan deaktiveres hvis det ikke er tillatt,. Det er også passordbeskyttet for å hindre uautorisert tilgang.

De fleste enhetsinnstillingene er tilgjengelige via RUI. Elementer som ikke kan konfigureres ved hjelp av dette grensesnittet, kan konfigureres i enhetens kontrollpanel. Vi anbefaler å deaktivere alle ubrukte tjenester og stramme inn kontrollene på dem som trengs. Operatørsettet for ekstern støtte gir ekstern tilgang til enhetens kontrollpanel for å gi fleksibilitet og støtte. Dette er basert på VNC-teknologi som består av en server (MFD) og en klient (en nettverks-PC). Et bestemt visningsprogram for Canon-klient-PC-en gir simulert tilgang til tastene på kontrollpanelet der det trengs.

Denne delen inneholder en oversikt over viktige sikkerhetsrelaterte funksjoner for imageRUNNER ADVANCE, og konfigurasjonsinnstillingene for dem.

Interaktive brukerhåndbøker på nett er å finne på https://oip.manual.canon/, med mer informasjon om sikkerhetsrelaterte funksjoner. Begynn med å velge riktig produkttype (f.eks. imageRUNNER ADVANCE DX), klikke på søkeikonet og skrive inn søkekriteriene. Nedenfor er noen generelle ting som er verdt å vurdere.

Administrering av maskinen

Konstante og effektive sikkerhetstiltak kreves for å hindre lekkasje av personlig informasjon eller uautorisert bruk. Ved å sette opp en administrator som håndterer enhetsinnstillingene, kan brukeradministrasjon og sikkerhetsinnstillinger begrenses til kun godkjente brukere.

Lim inn lenken nedenfor i nettleseren og skriv inn **administratorkonfigurasjon** i søkefeltet. Du vil da få frem informasjon om følgende:

- Grunnleggende administrasjon av enheten
- Begrensning av risiko ved uaktsomhet, brukerfeil og misbruk
- Enhetsbehandling
- Administrasjon av systemkonfigurasjon og innstillinger

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

IEEE P2600-standarden

En rekke imageRUNNER ADVANCE-modeller er IEEE P2600-kompatible. Dette er en global standard for informasjonssikkerhet for multifunksjonsenheter og skrivere.

I lenken nedenfor beskrives sikkerhetskravene som er definert i IEEE 2600-standarden, og hvordan enhetsfunksjonene oppfyller disse kravene.

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

IEEE 802.1X-autentisering

Ved tilkobling til et 802.1X-nettverk må enheten autentiseres for å sikre at den er en godkjent tilkobling.

Lim inn lenken nedenfor i nettleseren og skriv inn **802.1X** i søkefeltet.

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

Bruke en sikkerhetspolicy på maskinen

De nyeste imageRUNNER ADVANCE-modellene tillater administrering av flere sikkerhetsinnstillinger, sikkerhetspolicyen, via RUI. Det kan brukes et eget passord, slik at bare sikkerhetsadministratoren kan endre innstillingene.

Lim inn lenken nedenfor i nettleseren og skriv inn **Bruke en sikkerhetspolicy på maskinen** i søkefeltet. Du vil da få frem informasjon om følgende:

- Bruke et passord til å beskytte sikkerhetspolicyinnstillingene
- Konfigurere sikkerhetspolicyinnstillingene
- Elementer i sikkerhetspolicyinnstillingene

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

Administrasjon av brukere

Kunder som trenger økt sikkerhet og effektivitet, kan bruke innebygde funksjoner eller en løsning for administrasjon av utskrifter, for eksempel uniFLOW.

Hvis du vil ha mer informasjon om løsningene våre for administrasjon av utskrifter, kan du kontakte våre lokale representanter eller se uniFLOWs produktbrosjyre.

Konfigurering av innstillingene for nettverkssikkerhet

Autoriserte brukere kan oppleve uforutsette tap etter angrep fra skadelige tredjeparter, for eksempel sporing, forfalskning og tukling med data i nettverket. For å beskytte viktig og verdifull informasjon mot disse angrepene støtter maskinen en rekke funksjoner som forbedrer sikkerheten og personvernet.

Lim inn lenken nedenfor i nettleseren og skriv inn **konfigurering av innstillingene for nettverkssikkerhet** i søkefeltet. Du vil da få frem informasjon om følgende:

På lenken nedenfor finner du detaljer om følgende:

- Forhindre uautorisert tilgang
- Tilkobling til trådløst LAN
- Konfigurering av nettverksmiljøet

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

Administrasjon av data på harddisken

Enhetens harddisk brukes til å lagre enhetens operativsystem, konfigurasjonsinnstillinger og jobbinformasjon. På de fleste enhetsmodeller kan diskene krypteres helt (kompatibelt med FIPS 140-2) når de pares med den bestemte enheten, for å hindre at uautoriserte brukere leser dem. En forberedende Canon MFP-sikkerhetsbrikke er sertifisert som en kryptografisk modul under Cryptographic Module Validation Program (CMVP), som er etablert av USA og Canada samt Japan Cryptographic Module Validation Program (JCMVP).

Lim inn lenken nedenfor i nettleseren og skriv inn **administrasjon av data på harddisken** i søkefeltet.

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

SIKKERHETSPOLICYINNSTILLINGER – OVERSIKT

I tredje generasjons imageRUNNER ADVANCE-modeller innføres sikkerhetspolicyinnstillinger og sikkerhetsadministratorer. Dette krever at administratoren har logget seg på, og hvis konfigurert, pålogging med et ekstra passord for sikkerhetsadministrator.

Tabellen nedenfor inneholder mer informasjon om innstillingene.

1. Grensesnitt	Merknader
Policy for trådløs tilkobling	
Forby bruk av direkte tilkobling	<Bruk Wi-Fi Direct> er satt til <Av> Det er ikke mulig å gå inn på maskinen fra mobilenheter
Forby bruk av trådløst nettverk	<Velg kablet/trådløst nettverk> er satt til <Kablet nettverk> Det er ikke mulig å etablere en trådløs forbindelse til maskinen via en trådløs LAN-ruter eller et tilgangspunkt
Policy for USB	
Forby bruk som USB-enhet	<Bruk USB-enhet> er satt til <Av> Du vil ikke kunne bruke utskrifts- eller skannefunksjonene fra PC-er som er koblet til via USB når det er forbudt å bruke en USB-enhet
Forby bruk som USB-lagringsenhet	<Bruk USB-lagringsenhet> er satt til <Av> Det er ikke mulig å bruke USB-lagringsenheter Følgende tjenestefunksjoner fungerer likevel, selv om Forby bruk som USB-lagringsenhet er PÅ • Fastvareoppdatering med USB-minnepinne (fra nedlastingsmodus) • Kopiere sublog-data fra enheten til USB (LOG2USB) • Kopiere rapporten fra enheten til USB (RPT2USB)
Operasjonspolicy for nettverkskommunikasjon Merk: Disse innstillingene gjelder ikke for kommunikasjon med IEEE 802.1X-nettverk, selv om avmerkingsboksen er valgt for [Alltid bekreft serversertifikat ved bruk av TLS]	
Alltid bekreft signaturer for SMS/ WebDAV-serverfunksjoner	I <Innstillinger for SMB-server> er alternativet <Krev SMB-signatur for tilkobling> og <Bruk SMB-autentisering> satt til <På> og alternativet <Bruk TLS> i <Innstillinger for WebDAV-server> til <På> Digitale sertifikatsignaturer verifiseres under kommunikasjon når maskinen brukes som SMB-server eller WebDAV-server
Alltid kontroller serversertifikatet ved bruk av TLS	<Bekreft TLS-sertifikat for WebDAV TX>, <Bekreft TLS-sertifikat for SMTP TX>, <Bekreft TLS-sertifikat for POP RX>, <Bekreft TLS-sertifikat for nettverkstilgang> og <Bekreft TLS-sertifikat med MEAP-program> er satt til <På>, og det legges til et avkrysningsmerke i <CN> I tillegg settes alternativene <Bekreft serversertifikat> og <Bekreft CN> i <SIP-innstillinger> > <TLS-innstillinger> til <På> Under TLS-kommunikasjon kjøres det en verifisering for digitale sertifikater og vanlige navn for dem
Forby autentisering med klartekst for serverfunksjoner	• <Bruk FTP-utskrift> i <Innstillinger for FTP-utskrift> er satt til <Av> • <Tillat TLS (SMTP RX)> i <Innstillinger for e-post/i-Fax> <Kommunikasjonsinnstillinger> er satt til <Alltid TLS>, <Autentiseringsmetode for dedikert port> i <Nettverk> er satt til <modus 2>, • <Bruk TLS> i <Innstillinger for WebDAV-server> er satt til <På> Når du bruker maskinen som server, har du ikke tilgang til funksjoner som bruker autentisering med klartekst TLS brukes hvis autentisering med klartekst er forbudt. I tillegg kan du ikke bruke programmer eller serverfunksjoner, for eksempel FTP, som bare støtter autentisering med klartekst Det kan hende det ikke er mulig å gå inn på maskinen fra programvaren eller driveren for enhetsadministrasjon
Forby bruk av SNMPv1	I <SNMP Settings> settes <Bruk SNMPv1>til <Av> Det kan hende at du ikke kan hente inn eller angi enhetsinformasjon fra skriverdriveren eller programvaren for enhetsadministrasjon hvis det er forbudt å bruke SNMPv1
Policy for portbruk	
Begrens LPD-port	Portnummer: 515 <Innstillinger for LPD-utskrift> er satt til <Av> Det er ikke mulig å kjøre LPD-utskrifter
Begrens RAW-port	Portnummer 9100 <Innstillinger for RAW-utskrift> er satt til <Av> Det er ikke mulig å kjøre RAW-utskrifter
Begrens FTP-port	Portnummer 21 I <Innstillinger for FTP-utskrift> er <Bruk FTP-utskrift> satt til <Av> Det er ikke mulig å kjøre FTP-utskrifter
Begrens WSD-porten	Portnummer: 3702, 60000 I <WSD-innstillinger> settes alternativene <Bruk WSD>, <Bruk WSD-lesing> og <Bruk WSD-skann> alle til <Av> WSD-funksjonene kan ikke brukes

Begrens BMLinkS-port	Portnummer 1900 Brukes ikke i Europa
Begrens IPP-porten	Portnummer 631 Du kan ikke bruke Mopria, AirPrint og IPP hvis IPP-porten er begrenset
Begrens SMB-port	Portnummer: 137, 138, 139, 445 I <Innstillinger for SMB-server> er <Bruk SMB Server> satt til <Av> Maskinen kan ikke brukes som SMB-server
Begrens SMTP-port	Portnummer 25 I <Innstillinger for e-post/i-Fax> > <Kommunikasjonsinnstillinger> er <SMTP RX> satt til <Av> Mottak av SMTP er ikke mulig
Begrens dedikert port	Portnummer: 9002, 9006, 9007, 9011–9015, 9017–9019, 9022, 9023, 9025, 20317, 47545–47547 Du kan ikke bruke funksjonene for ekstern kopiering, ekstern faks, ekstern skanning eller ekstern utskrift, eller programmer osv., hvis den dedikerte porten er begrenset
Begrens porten for programvare for ekstern operatør	Portnummer 5900 <Innstillinger for Fjernbetjening> er satt til <Av> Fjernbetjeningsfunksjoner kan ikke brukes
Begrens SIP-port (IP-faks)	Portnummer: 5004, 5005, 5060, 5061, 49152) <Bruk Intranet> i <Innstillinger for Intranet>, <Bruk NGN> i <NGN-innstillinger> og <Bruk VoIP-gateway> i <Innstillinger for VoIP-gateway> er alle satt til <Av> IP-faks kan ikke brukes
Begrens mDNS-port	Portnummer 5353 I <mDNS Settings> er alternativene <Bruk IPv4 mDNS> og <Bruk IPv6 mDNS> satt til <Av> <Bruk Mopria> er satt til <Av> Det går ikke an å søke i nettverket eller utføre automatiske innstillinger ved hjelp av mDNS. Det går heller ikke an å skrive ut ved hjelp av Mopria™ eller AirPrint
Begrens SLP-port	Portnummer 427 I <Innstillinger for Multicast Discovery> er <Svar> satt til <Av> Det går ikke an å søke i nettverket eller utføre automatiske innstillinger ved hjelp av SLP
Begrens SNMP-port	Portnummer 161 Det kan hende at du ikke kan hente inn eller angi enhetsinformasjon fra skriverdriveren eller programvaren for enhetsadministrasjon hvis SNMP-porten er begrenset I <SNMP-innstillinger> er alternativene <Bruk SNMPv1> og <Bruk SNMPv3> satt til <Av>

2. Autentisering	Merknader
Operasjonspolicy for autentisering	
Forby gjestebrukere	• <Innstillinger for Advanced Space> > <Administrasjon av autentisering> er satt til <På> • <Skjerminnstillinger for pålogging> er satt til <Vis når enhetsoperasjonen starter> • <Begrens jobb fra ekstern enhet uten brukerautentisering> er satt til <På> Uregistrerte brukere kan ikke logge på maskinen, og utskriftsjobber som sendes fra en datamaskin, avbrytes
Tving innstilling for automatisk avlogging	Denne innstillingen brukes for å logge av kontrollpanelet. Dette gjelder ikke for andre avloggingsmetoder (område som kan stilles inn: 10 sekunder–9 minutter) <Tid for automatisk tilbakestilling> er aktivert. Brukeren logges automatisk av hvis ingen operasjoner utføres i en angitt tidsperiode Velg [Tid til avlogging] på skjermbildet med innstillinger for eksternt brukergrensesnitt
Operasjonspolicy for passord	
Forby bufring av passord for eksterne servere	Denne innstillingen gjelder ikke for passord som brukeren uttrykkelig lagrer, for eksempel passord for adressebøker osv. Forby bufring av autentiseringspassord> er satt til <På> Brukere må alltid angi et passord når de skal bruke en ekstern server
Vis advarsel når standardpassord er i bruk	<Vis advarsel når standardpassord er i bruk> er satt til <På> Det vises en advarsel hver gang maskinens fabrikkinnstilte passord brukes
Forbyr bruk av standardpassord for ekstern tilgang	<Tillat bruk av standardpassord for ekstern tilgang> er satt til <Av> Standardpassordet fra fabrikkinnstillingene kan ikke brukes når man går inn på maskinen fra en datamaskin
Policy for passordinnstillinger (policyen gjelder ikke for administrasjon av avdelings-ID eller PIN-kode)	
Angi minimum antall tegn for passord	Minimum antall tegn for passord kan settes til mellom 1 og 32
Angi gyldighetsperiode for passord	Gyldighetsperioden kan settes til mellom 1 og 180 dager
Forby bruk av tre eller flere identiske tegn etter hverandre	
Tvinge bruk av minst én stor bokstav	
Tvinge bruk av minst én liten bokstav	
Tving bruk av minst ett siffer	
Tving bruk av minst ett symbol	
Policy for lockout	
Aktiver lockout	Gjelder ikke for avdelings-ID / PIN-kode for postboks, PIN-kode eller sikker utskrift-autentisering osv. Grense for lockout: kan settes til mellom 1 og 10 ganger Blokkeringsperiode: kan settes til mellom 1 og 60 minutter

3. Nøkkel/sertifikat	Merknader
Forby bruk av svak kryptering	Gjelder for IPSec, TLS, Kerberos, S/MIME, SNMPv3 og trådløst LAN Det kan hende du ikke kan kommunisere med enheter som kun støtter svak kryptering
Forby bruk av nøkkel/sertifikat med svak kryptering	Gjelder for IPSec, TLS og S/MIME Hvis du bruker en nøkkel / et sertifikat med svak kryptering for TLS, endres det til den forhåndsinstallerte nøkkelen/sertifikatet. Du kan ikke kommunisere hvis du bruker en nøkkel / et sertifikat med svak kryptering for andre funksjoner enn TLS
Bruk TPM til å lagre passord og nøkkel	Kun tilgjengelig for enheter TPM er installert på. Alltid sikkerhetskopier TPM-nøklene når TPM er aktivert. Se brukerhåndboken for mer informasjon Viktig når TPM-innstillinger er aktivert • Pass på at du endrer administratorpassordet fra standardverdien for å hindre at tredjeparter som ikke er administrator, kan sikkerhetskopiere TPM-nøkkelen. Du kan ikke gjenopprette TPM-nøkkelen hvis en tredjepart får tak i den sikkerhetskopierte TPM-nøkkelen • Av hensyn til sikkerhet kan TPM-nøkkelen sikkerhetskopieres kun én gang. Hvis TPM-innstillingene er aktivert, må du sikkerhetskopiere TPM-nøkkelen på en USB-minneenhet og oppbevare minneenhet på et trygt sted for å unngå at den mistes eller blir stjålet • Sikkerhetsfunksjonene i TPM garanterer ikke full beskyttelse av data og maskinvare

4. Logg	Merknader
Tvungen registrering av revisjonslogg	• <Lagre operasjonslogg> er satt til <På> • <Vis jobblogg> er satt til <På> • <Hent jobblogg med administrasjonsprogramvare> i <Vis jobblogg> er satt til <Tillat> • <Lagre revisjonslogg> er satt til <På> • <Hent autentiseringslogg for nettverket> er satt til <På> Revisjonslogger registreres alltid når denne innstillingen er aktivert
Tving SNTP-innstillinger	Angi adresse for SNTP-server I <SNTP-innstillinger> er <Bruk SNTP> satt til <På> Tidssynkronisering via SNTP er obligatorisk Angi en verdi for [Servernavn] på innstillingsskjermen i det eksterne brukergrensesnittet
Rapportering av Syslog-logg	Aktiver målinformasjon for Syslog når det brukes en Syslog-server eller SIEM • <Brukernavn og passord> • <SMB-servernavn> • <Målbane> • <Kjør eksporttid>

5. jobb	Merknader
Utskriftspolicy	
Forhindrer umiddelbar utskrift av mottatte jobber	Mottatte jobber lagres i faks-/I-Fax-minnet hvis det ikke er tillatt å skrive ut mottatte jobber umiddelbart • <Behandle filer med videresendingsfeil> er satt til <Av> • <Bruk minnelås for faks> er satt til <På> • <Bruk minnelås for I-Fax> er satt til <På> • <Sluttid for minnelås> er satt til <Av> • <Vis utskrift ved lagring fra skriverdriver> i <Angi/registrer konfidensielle faksinnbokser> er satt til <Av> • <Innstillinger for alle postbokser> > <Skriv ut ved lagring fra skriverdriver> er satt til <Av> • <Sikkerhetsinnstillinger for boks> > <Vis utskrift ved lagring fra skriverdriver> er satt til <Av> • <Forby jobb fra ukjent bruker> er satt til <På>, og <Tvungen holding> er satt til <På> Utskriften skjer ikke umiddelbart, selv når det kjøres utskriftsoperasjoner
Policy for sending/mottak	
Tillat sending kun til registrerte adresser	I <Begrens ny mottaker> er alternativene <Faks>, <E-post>, <I-Fax> og <Fil> satt til <På> Det går kun an å sende til mottakere som er registrert i adresseboken
Tving bekreftelse av faksnummer	Brukerne må angi et faksnummer på nytt for å få en bekreftelse når de sender faks.
Forby automatisk videresending	<Bruk automatisk videresending> er satt til <Av> Det går ikke an å videresende fakser automatisk

6. Oppbevaring	Merknader
Tving fullstendig sletting av data	<Fullfør sletting av harddiskdata> er satt til <På>

Hvis du ønsker fullstendige spesifikasjoner for imageRUNNER ADVANCE, ber vi deg gå til webområdet for produktet på https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Norge AS
Hallagerbakken 110
Postboks 33 Holmlia
1201 OSLO
Tlf. +47 2262 9200
canon.no

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Norwegian edition v1.0