MFD-SÄKERHETSGUIDE

imageRUNNER ADVANCE

Canon

INLEDNING

Moderna multifunktionsenheter (MFD:er) från Canon med funktioner för utskrift, kopiering, scanning, sändning och fax. MFD:er är datorservrar på sitt eget sätt och kan tillhandahålla ett antal nätverksbaserade tjänster och stor hårddisklagring.

När en organisation inför dessa enheter i infrastrukturen finns det ett antal områden som bör övervägas inom den bredare säkerhetsstrategin vars mål ska vara att skydda sekretessen, integriteten och tillgängligheten för ditt nätverkssystem.

Distributionen varierar naturligtvis och organisationer har sina egna specifika säkerhetskrav. Samtidigt som vi arbetar tillsammans för att säkerställa att Canon-enheter levereras med lämpliga första säkerhetsinställningar strävar vi efter att möjliggöra det genom att tillhandahålla konfigurationsinställningar som gör att du kan anpassa enheten mer till kraven för din specifika situation.

Det här dokumentet är utformat för att tillhandahålla tillräckligt med information för att du ska kunna diskutera de mest lämpliga inställningarna för din miljö med Canon eller en Canon-partner. Vi vill uppmärksamma att inte alla enheter har samma kapacitet och olika systemprogramvaror kan erbjuda olika funktioner. När den slutliga konfigurationen har fastställts kan den tillämpas på din enhet eller maskinpark. Du kan kontakta Canon eller en Canon-partner för mer information och support.

Vem är det här dokumentet riktat till?

Det här dokumentet riktar sig till alla som bryr sig om multifunktionsenheters (MFD) utformning, implementering och säkerhet i en nätverksinfrastruktur. Det kan omfatta IT- och nätverksspecialister, IT-säkerhetspersonal och servicepersonal.

Omfattning

I den här guiden förklaras och rekommenderas konfigurationsinställningar för två vanliga nätverksmiljöer, så att organisationer kan implementera en MFD-lösning på ett säkert sätt baserat på bästa praxis. Dessutom förklaras (från version 3.8 av systemprogramvarans plattform) hur Syslog-funktionen kan ge feedback i realtid från MFD:n. De här inställningarna har testats och godkänts av Canons säkerhetsteam.

Vi gör inga antaganden om specifika bestämmelser för olika branscher som kan innebära andra säkerhetsanpassningar och som inte omfattas av det här dokumentet.

Den här guiden skapades utifrån den vanliga funktionsuppsättningen på imageRUNNER ADVANCE-plattformen och även om all information här gäller för alla modeller och serien i imageRUNNER ADVANCE-sortimentet kan vissa funktioner variera mellan modeller.

Implementera lämplig MFD-säkerhet för din miljö

Vi har tagit hänsyn till två vanliga scenarion för att utforska säkerhetskonsekvenserna av att implementera en multifunktionsenhet som en del av nätverket:

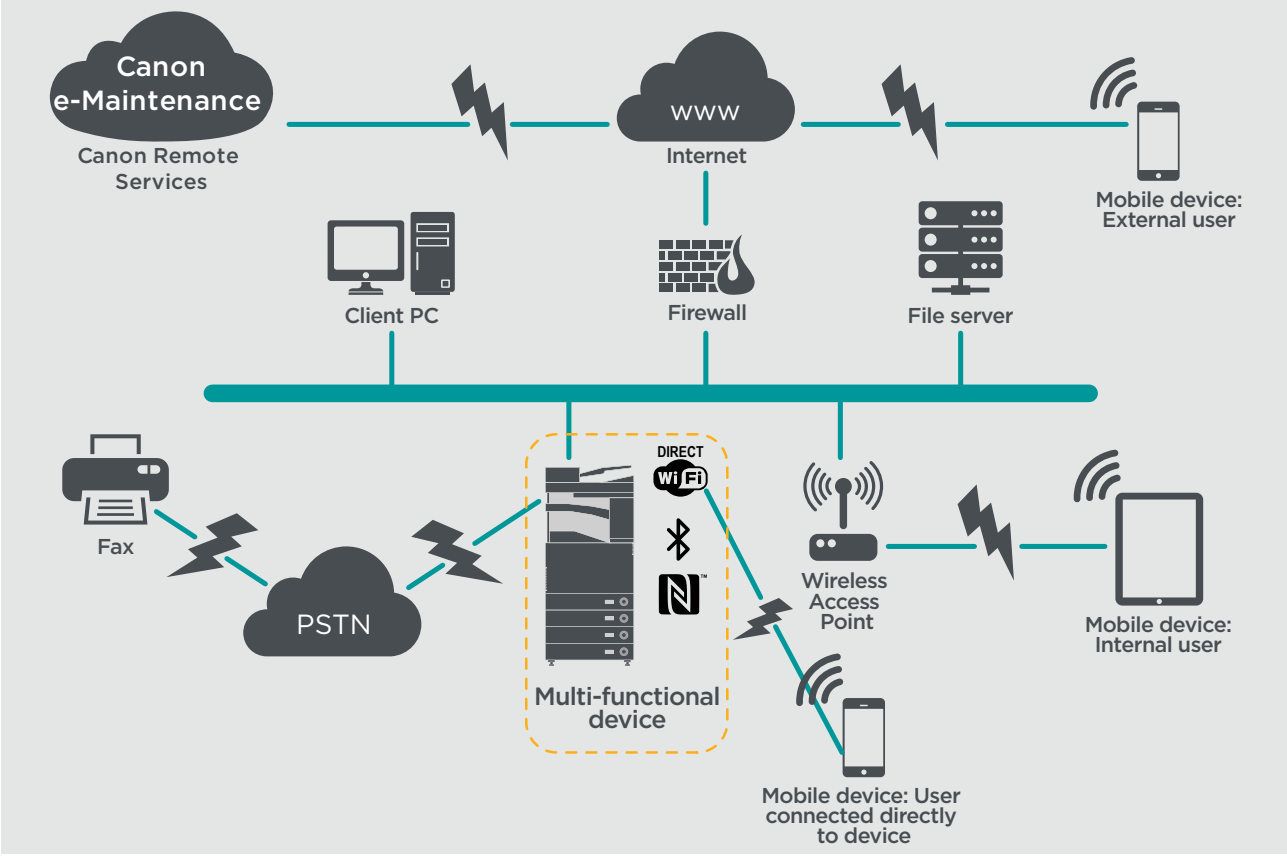
- **En vanlig miljö på ett litet kontor**
- **En miljö på ett stort företagskontor**

MILJÖ PÅ ETT LITET KONTOR

Vanligtvis är det här en miljö på ett litet företag med en nätverkstopologi utan segment. Det finns en eller två MFD:er för internt bruk och de är inte tillgängliga via internet.

Mobil utskrift är tillgänglig, men ytterligare lösningskomponenter krävs. För användare som behöver skrivartjänster utanför en LAN-miljö krävs en säker anslutning, med det ingår inte i den här guiden. Men det är viktigt att tänka på att skydda data som överförs mellan fjärrenheten och infrastrukturen för utskrifter.

Bild 1 Nätverk på små kontor



Den senaste generationens imageRUNNER ADVANCE-modeller har trådlös nätverksanslutning, vilket innebär att enheten kan anslutas till ett Wi-Fi-nätverk. Den kan även användas till att upprätta en WiFi Direct-anslutning mellan två punkter med en mobil enhet utan en nätverksanslutning.

Alternativen Bluetooth och NFC är tillgängliga för flera enhetsmodeller och används för att upprätta WiFi Direct-anslutningen för iOS- och Android-enheter.

ATT TÄNKA PÅ MED KONFIGURATIONEN

Observera att om en funktion hos imageRUNNER ADVANCE inte nämns nedan anses den vara tillräcklig med standardinställningarna för den här företags- och nätverksmiljön.

Tabell 1 Att tänka på med konfigurationen i en miljö på ett litet kontor

Funktion hos imageRUNNER ADVANCE	Beskrivning	Att tänka på
Serviceläge	Tillåter åtkomst till inställningarna för serviceläget	Skydda med ett ovanligt lösenord av maximal längd
Tjänstehanteringssystem	Tillåter åtkomst till flera enhetsinställningar som inte är standard	Skydda med ett ovanligt lösenord av maximal längd
SMB bläddra/skicka	Lagra och hämta till och från delade Windows-/SMB-nätverk	Systemadministratörer ska enligt policy inte låta användare skapa lokala konton på sin klientmaskin för att använda till att dela dokument med imageRUNNER ADVANCE över SMB
Fjärranvändargränssnitt	Webbaserat konfigurationsverktyg	Administratören för imageRUNNER ADVANCE ska aktivera HTTPS för fjärranvändargränssnittet och avaktivera HTTP-åtkomst. Aktivera användningen av autentisering med PIN-kod som är unik för varje enhet
SNMP	Integrering av nätverksövervakning	Avaktivera version 1 och aktivera endast version 3
Skicka till e-post eller IFAX	Skicka e-postmeddelanden från enheten med bilagor	Aktivera SSL Använd inte POP3-autentiseringen innan du skickar med SMTP Använd SMTP-autentisering
POP3	Hämta och skriv ut dokument automatiskt från brevlådan	Aktivera SSL Aktivera POP3-autentisering
Adressbok/LDAP	Använd katalogtjänsten för att söka hemnummer eller e-postadresser att skicka scanningar till	Aktivera SSL Använd inte domäninloggningsuppgifter för att autentisera mot LDAP-servern. Använd LDAP-specifika inloggningsuppgifter
FTP-utskrift	Överför och hämta dokument till och från den inbyggda FTP-servern	Sätt på FTP-autentisering. Tänk på att FTP-trafik alltid överförs i klartext över nätverket
WebDAV Send	Scanna och lagra dokument på en annan plats	Aktivera autentisering för WebDAV-delningar
Krypterad PDF	Kryptera dokument	Enligt policy ska känsliga dokument endast krypteras med PDF-versionen 1.6 (AES-128)
Säkra utskrifter	Utskriftsjobb skickas till enheten, men stannar i utskriftskön tills motsvarande PIN-kod anges	Aktivera utskriftsjobb som skyddas av PIN-kod
Händelseavisering för Syslog	Systemloggningsprotokoll är ett protokoll enligt branschstandard som används för att skicka meddelanden om systemloggar eller händelser till en specifik server som kallas för en Syslog-server	Överväg att rikta Syslog-data för imageRUNNER till ditt befintliga Syslog-analysverktyg i nätverket eller företagets SIEM-plattform (Security Event Management System).
Systemverifiering vid start	Kontrollerar att systemets programvarukomponenter inte har försämrats. Det påverkar tiden för systemets uppstart minimalt	Aktivera funktion
Inbyggd webbläsare	Åtkomst till internet via webbläsare	Via administration kan användningen av en webbproxy som filtrerar innehåll tillämpas för att undvika åtkomst till skadligt eller viralt innehåll. Avaktivera alternativet att skapa favoriter
Bluetooth och NFC (tillgänglig från Generation 3-modeller)	Används för att upprätta en WiFi Direct-anslutning	Aktivera WiFi Direct för att tillåta direktanslutning till en mobil enhet. WiFi Direct kan inte användas när Wi-Fi används för att ansluta till ett nätverk
Trådlös LAN-	Ger trådlös åtkomst	Använd WPA-PSK/WPA2-PSK med starka lösenord
IPP	Anslut och skicka utskriftsjobb över IP	Avaktivera IPP

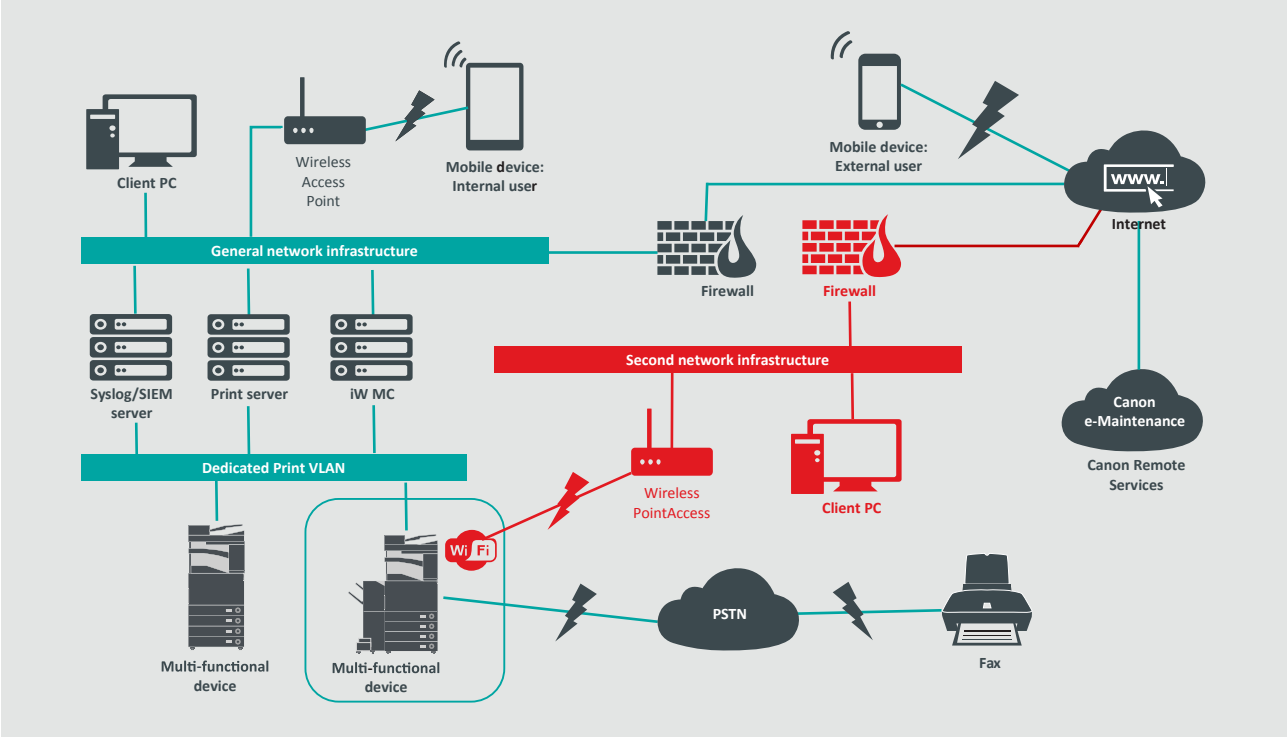
EN MILJÖ PÅ ETT STORT FÖRETAGSKONTOR

Det här är vanligtvis en miljö som spänner över flera platser och flera kontor, med segmenterad nätverksarkitektur. Den har flera MFD:er distribuerade på ett separat VLAN som är tillgängligt för intern användning via utskriftsservrar. MFD:erna är inte tillgängliga från internet.

Den här miljön har oftast ett permanent team som hanterar nätverkskrav och administrativa krav samt allmänna datorproblem, men teamet förväntas inte ha någon specifik MFD-utbildning.

Det här är vanligtvis en miljö som spänner över flera platser och flera kontor, med segmenterad nätverksarkitektur. Den har flera MFD:er distribuerade på ett separat VLAN som är tillgängligt för intern användning via utskriftsservrar. MFD:erna är inte tillgängliga från internet.

Bild 2 Arbete på företagskontor



Anslutningar markerade i rött är tillgängliga från Generation 3-modeller

ATT TÄNKA PÅ MED KONFIGURATIONEN

Observera att om en funktion hos imageRUNNER ADVANCE inte nämns nedan anses den vara tillräcklig med standardinställningarna för den här företags- och nätverksmiljön.

Tabell 2 Att tänka på med konfigurationen i en miljö på ett stort företagskontor

Funktion hos imageRUNNER ADVANCE	Beskrivning	Att tänka på
Serviceläge	Tillåter åtkomst till inställningarna för serviceläget	Skydda med ett ovanligt lösenord av maximal längd
Tjänstehanteringssystem	Ger åtkomst till flera enhetsinställningar som inte är standard	Skydda med ett ovanligt lösenord av maximal längd
SMB bläddra/skicka	Lagra och hämta till och från delade Windows-/SMB-nätverk	Systemadministratörer ska enligt policy inte låta användare skapa lokala konton på sin maskin för att använda till att dela dokument med imageRUNNER ADVANCE över SMB
Fjärranvändargränssnitt	Webbaserat konfigurationsverktyg	Om du följer de första enhetskonfigurationerna avaktiveras fjärranvändargränssnittet helt genom att HTTP och HTTPS avaktiveras
SNMP	Integrering av nätverksövervakning	Avaktivera version 1 och aktivera endast version 3
Skicka till e-post eller IFAX	Skicka e-postmeddelanden från enheten med bilagor	Aktivera SSL Aktivera: – Certifikatverifiering på SMTP-servern Eller om det inte är gångbart: – Använd endast den här funktionen i en miljö som har en insamlare för system med inkräktaravkänning i nätverket Använd inte POP3-autentiseringen innan du skickar med SMTP Använd SMTP-autentisering
POP3	Hämta och skriv ut dokument automatiskt från brevlådan	Aktivera SSL Aktivera: – Certifikatverifiering på POP3-servern Eller om det inte är gångbart: – Använd endast den här funktionen i en miljö som har en insamlare för system med inkräktaravkänning i nätverket Aktivera POP3-autentisering
Adressbok/LDAP	Använd katalogtjänsten för att söka telefonnummer eller e-postadresser att skicka scanningar till	Aktivera SSL Aktivera: – Certifikatverifiering på LDAP-servern Eller om det inte är gångbart: – Använd endast den här funktionen i en miljö som har en insamlare för system med inkräktaravkänning i nätverket Använd inte domäninloggningsuppgifter för att autentisera mot LDAP-servern. Använd LDAP-specifika inloggningsuppgifter
IPP	Anslut och skicka utskriftsjobb över IP	Avaktivera IPP
WebDAV Send	Scanna och lagra dokument på en annan plats	Aktivera autentisering för WebDAV-delningar Aktivera SSL Tvinga skrivaren att endast tillåta filer som slutar med ”filutskriftstillägg” att överföras
IEEE802.1X	Autentiseringsmekanism för nätverksåtkomst	Stöd för EAPOL V1
Krypterad PDF	Kryptera dokument	Enligt policy ska känsliga dokument endast krypteras med PDF-versionen 1.6 (AES-128)
Krypterad säker utskrift	Utöka skyddet från säker utskrift genom att kryptera filen och lösenordet under överföring	Konfigurera användarnamnet på fliken Skrivare i klientskrivarens konfiguration till ett annat användarnamn än LDAP-/domäninloggningsuppgifterna för den användaren. Kontrollera att ”Begränsa utskriftsjobb” är av
Automatisk certifikatregistrering	Den automatiska registreringen förbättrar effektiviteten vid hämtning och distribution av digitala certifikat	Kräver en nätverkscertifikatlösning för att kunna användas
Händelseavisering för Syslog	Systemloggningsprotokoll är ett protokoll enligt branschstandard som används för att skicka meddelanden om systemloggar eller händelser till en specifik server som kallas för en Syslog-server	Överväg att rikta Syslog-data för imageRUNNER ADVANCE till ditt befintliga Syslog-analysverktyg i nätverket eller företagets SIEM-plattform (Security Event Management System)
Systemverifiering vid start	Kontrollerar att systemets programvarukomponenter inte har försämrats. Det påverkar tiden för systemets uppstart minimalt	Aktivera funktion
Trådlöst LAN	Ger trådlös åtkomst	Använd WPA-PSK/WPA2-PSK med starka lösenord
WiFi Direct	Används för att upprätta en WiFi Direct-anslutning	Avaktivera WiFi Direct
Inbyggd webbläsare (tillgänglig från Generation 3-modeller i andra utgåvan)	Åtkomst till internet via webbläsare	Tillämpa lämpliga begränsningar eller avaktivera alternativet att hämta filer via webbläsaren

Den senaste generationens imageRUNNER ADVANCE-modeller har trådlös nätverksanslutning, vilket innebär att enheten kan anslutas till ett Wi-Fi-nätverk samtidigt som den är ansluten till ett trådbundet nätverk. Det här scenariot kan vara användbart när kunden behöver dela en enheten över två nätverk. En skolmiljö är ett vanligt exempel där det finns separata nätverk för anställda och elever.

imageRUNNER ADVANCE-plattformen tillhandahåller en funktionsmiljö för flexibel användning. Med protokollen och tjänsterna som är tillgängliga för att möjliggöra detta är det viktigt att se till att endast de funktioner, tjänster och protokoll som krävs är aktiva för att tillgodose användarens behov. Det här är en bra säkerhetspraxis och minskar den potentiella attackytan och förhindrar exploatering. Eftersom det ständigt dyker upp nya sårbarheter måste vi alltid vara försiktiga med att kompromissa, oavsett om det är direkt kopplat till enheten eller inte. Det är användbart att kunna övervaka användaraktiviteten för att kunna identifiera och vidta korrigerande åtgärder vid behov.

Version 3.8 av plattformen för programvaran imageRUNNER ADVANCE har ytterligare funktioner utöver de som har varit tillgängliga i flera år. Det är bland annat möjligheten att övervaka enheten i realtid med hjälp av Syslog och systemverifiering vid start. Genom att använda de här funktionerna tillsammans med dina befintliga nätverkssäkerhetslösningar, till exempel en SIEM-plattform (Security Information Event Management) eller loggningslösning, får du större översikt och identifiering av incidenter och tekniska undersökningar.

Systemverifiering vid start

Den här funktionen är en maskinvarumekanism som är utformad för att kontrollera att alla delar i systemprogramvaran imageRUNNER ADVANCE Generation 3 3rd Edition verifieras mot en ROT (Root of Trust) för att säkerställa att operativsystemet laddar som Canon avser. Om en skadlig part modifierar eller försöker modifiera systemet, eller om ett fel inträffar när systemet laddas stoppas processen och en felkod visas.

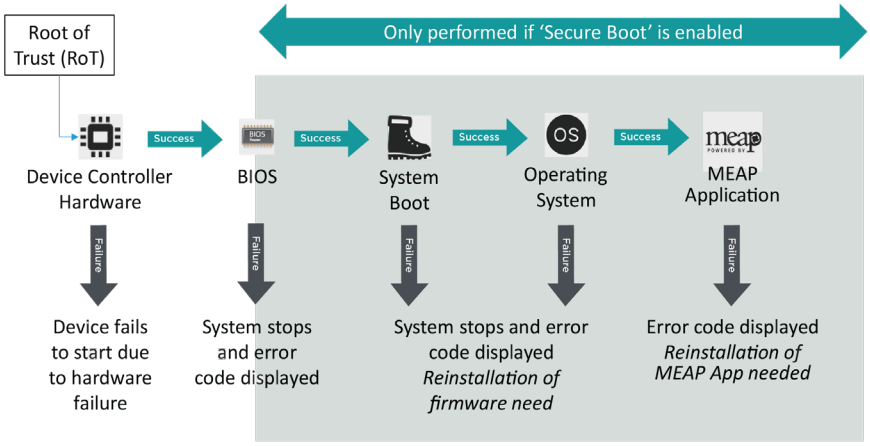


Bild 3 Process för systemverifiering vid start

Processen är transparent för användaren, förutom skärmen som visar att en obehörig systemversion laddas. imageRUNNER ADVANCE Generation 3 3rd Edition har ett alternativ för att aktivera systemverifiering vid start som ska vara påslaget för att aktivera den här säkerhetsfunktionen.

Automatisk certifikatregistrering

I de tidigare versionerna än 3.8 av plattformen för systemprogramvaran imageRUNNER ADVANCE var administratören tvungen att manuellt installera uppdaterade säkerhetscertifikat på varje enhet.
Det är en mödosam uppgift eftersom du måste ansluta till varje enhet för att kunna utföra en manuell uppdatering – certifikat måste uppdateras manuellt med hjälp av det specifika fjärranvändargränssnittet (RUI) för enheter, vilket gör att processen tar mycket längre tid.
Med tjänsten automatisk certifikatregistrering som införs från version 3.8 och senare av plattformen har den här fasta kostnaden tagits bort.

Den automatiska registreringen förbättrar effektiviteten vid hämtning certifikat. Den gör det möjligt att automatiskt hämta certifikat med hjälp av NDES (Network Device Enrolment Service) för Microsoft Windows och SCEP (Simple Certificate Enrolment Protocol).

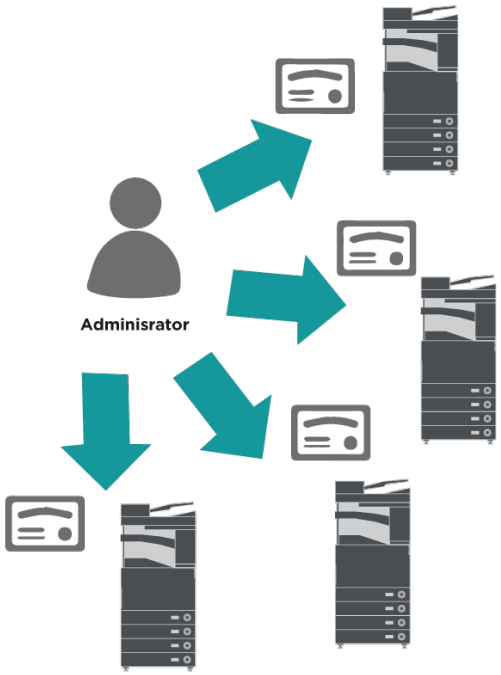


Bild 4 Certifikatregistrering

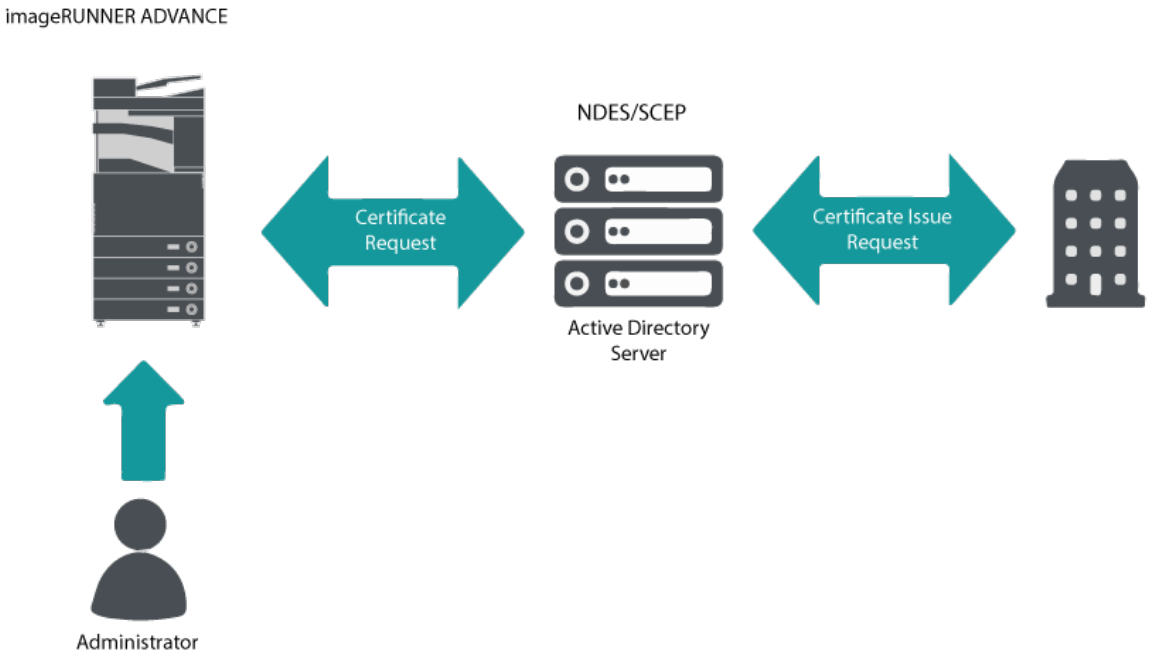


Bild 5 Process för certifikatregistrering

SCEP är ett protokoll som har stöd för certifikat utfärdade av en certifikatutfärdare (CA) och NDES gör att nätverksenheter kan hämta eller uppdatera certifikat baserat på SCEP.

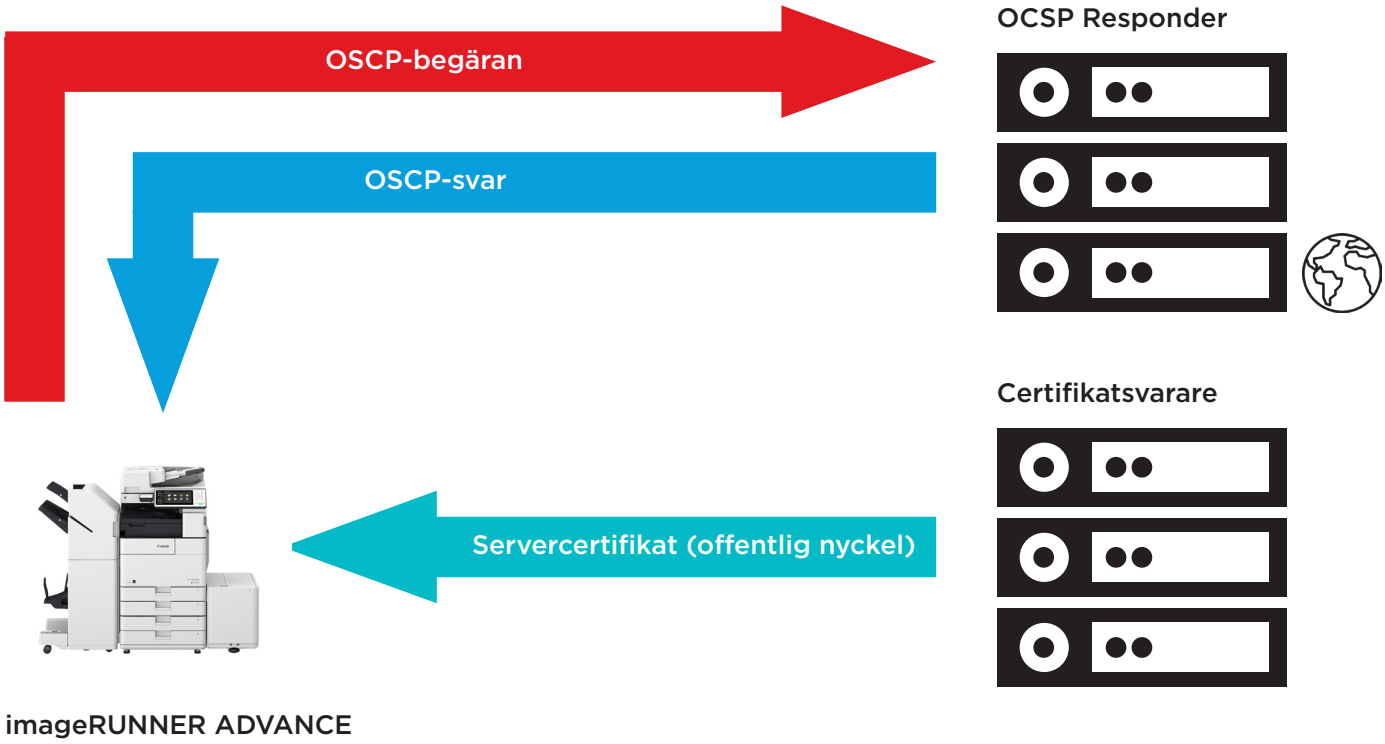
NDES är en rolltjänst i Active Directory-certifikattjänsterna.

Online Certificate Status Protocol

Det finns flera anledningar till varför det kan vara nödvändigt att återkalla ett digitalt certifikat. Det kan krävas om till exempel den privata nyckeln har tappats bort, blivit stulen, kompromissats eller om ett domännamn har ändrats.

OCSP (Online Certificate Status Protocol) är ett standardinternetprotokoll som används för att kontrollera återkallningsstatusen för ett digitalt X.509-certifikat som har tillhandahållits av certifikatservern. Genom att skicka en OCSP-begäran till OCSP Responder (vanligtvis en certifikatutfärdare) och ange ett specifikt certifikat svarar OCSP Responder med ”bra”, ”återkallat” eller ”okänt”.

Bild 6 Process för OCSP-handskakning



Med imageRUNNER ADVANCE från version 3.10 av plattformen tillhandahåller OCSP en mekanism i realtid för att verifiera de installerade digitala X.509-certifikaten. Tidigare versioner av plattformen hade endast stöd för CRL-metoden (Certificate Revoke List), vilket är otillräckligt och resulterar i höga fasta kostnader för nätverksresurser.

Säkerhetsinformation och händelsehantering

Med imageRUNNER ADVANCE-tekniken är det möjligt att skicka ut säkerhetshändelser i realtid med hjälp av Syslog-protokollet som följer RFC 5424, RFC 5425 och RFC 5426.

Protokollet används av flera olika enhetstyper som ett sätt att samla in information i realtid som kan användas för att identifiera potentiella säkerhetsproblem.

För att underlätta identifieringen av hot och säkerhetsincidenter måste enheten konfigureras till att riktas till en SIEM-server (Security Incident Event Management) från tredje part.

Syslog-händelser som produceras av enheten kan användas för att skapa åtgärder via insamlingen i realtid och analys av händelser från flera olika kontextuella datakällor (bild 7). Det finns även stöd för efterlevnadsrapportering och incidentundersökning genom att använda ytterligare lösningar som en SIEM-server. Se exempel i bild 8.

Den senaste generationens imageRUNNER ADVANCE-enheter har Syslog-funktioner med stöd för en mängd händelser som kan samlas in. Det kan användas för att korrelera och analysera händelser över flera åtskilda källor för att identifiera trender eller avvikelser.

Bild 7 Hämtning av Syslog-data

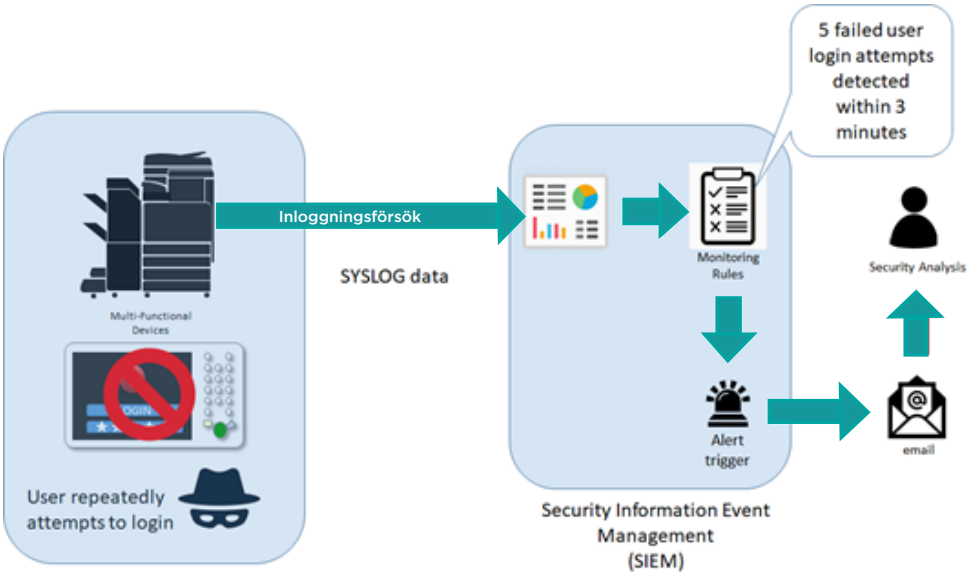


Bild 8 Exempel på användning av Syslog-data med imageRUNNER ADVANCE

Hantering av enhetsloggar

Utöver Syslog-funktionerna från version 3.8 av plattformen för systemprogramvaran har imageRUNNER ADVANCE följande loggar som kan hanteras på enheten. Loggarna kan exporteras i CSV-filformat via fjärranvändargränssnittet (RUI).

Tabell 3 – Exempel på loggfiler som kan hanteras av multifunktionsenheten.

Loggtyp	Nummer som visas som ”loggtyp” i CSV-filen	Beskrivning
Logg	4098	Den här loggen innehåller information relaterad till autentiseringsstatusen för användarautentiseringen (inloggning/utloggning och lyckad/misslyckad användarautentisering), registreringen/ändringen/borttagningen av användarinformation som hanteras med användarautentisering och hanteringen (lägga till/redigera/ta bort) av roller med ACCESS MANAGEMENT SYSTEM
Jobblogg	1001	Den här loggen innehåller information relaterad till slutförandet av kopiering/fax/scanning/sändning/utskrift
Överföringslogg	8193	Loggen innehåller information relaterad till överföringar
Logg för spara till avancerat utrymme	8196	Den här loggen innehåller information relaterad till att spara filer till det avancerade utrymmet, nätverket (avancerat utrymme i andra maskiner) och minnesenhet
Logg för brevlådeåtgärder	8197	Den här loggen innehåller information relaterad till åtgärderna som utförs i brevlådan, Memory RX-inkorgen och den skyddade faxinkorgen
Logg för brevlådeautentisering	8199	Den här loggen innehåller information relaterad till autentiseringsstatusen för brevlådan, Memory RX-inkorgen och den skyddade faxinkorgen
Logg för åtgärder i avancerat utrymme	8201	Den här loggen innehåller information relaterad till dataåtgärder i det avancerade utrymmet
Logg för maskinhantering	8198	Den här loggen innehåller information relaterad till påslagning/avstängning av maskinen, ändringar av inställningarna via (Settings/Registration) (Inställningar/Registrering), ändringar av inställningarna via funktionen för leverans av enhetsinformation och tidsinställningen för loggen för maskinhantering registrerar ändringar av användarinformation eller säkerhetsrelaterade inställningar när maskinen undersöks eller repareras av din lokala auktoriserade Canon-återförsäljare
Logg för nätverksautentisering	8200	Den här loggen registreras när IPSec-kommunikation misslyckas
Logg för exportera/importera alla	8202	Den här loggen innehåller information relaterad till import/export av inställningar via funktionen Exportera alla/importera alla
Logg för säkerhetskopia av brevlåda	8203	Den här loggen innehåller information relaterad till säkerhetskopior av data i användarinkorgarna, Memory RX-inkorgen, den skyddade faxinkorgen, det avancerade utrymmet och eventuella lagrade data samt formuläret som registrerades för funktionen överlagra bilder
Logg för åtgärder för hantering av program/programvara	3101	Det här är en åtgärdslogg för SMS (Service Management Service), registrering/uppdatering av programvara och installationsprogram för MEAP-programvara osv.
Logg för säkerhetspolicy	8204	Den här loggen innehåller information relaterad till inställningsstatusen för säkerhetspolicyinställningarna
Logg för grupphantering	8205	Den här loggen innehåller information relaterad till inställningsstatusen (registrera/redigera/ta bort) för användargrupperna
Logg för systemunderhåll	8206	Den här loggen innehåller information relaterad till uppdateringar av den inbyggda programvaran och säkerhetskopiering/återställning av MEAP-programvaran osv.
Logg för autentiseringsutskrift	8207	Den här loggen innehåller information och åtgärdshistorik relaterade till vänteläge för utskrifter
Logg för inställningssynkronisering	8208	Den här loggen innehåller information relaterad till synkroniseringen av maskininställningar. Synkronisera inställningar för flera multifunktionsskrivare från Canon
Logg för hantering av granskningslogg	3001	Den här loggen innehåller information relaterad till början och slutet av den här funktionen (funktionen hantering av granskningslogg), samt export av loggar osv.

Loggar kan innehålla upp till 40 000 register. När antalet register överskrider 40 000 raderas de äldsta registren först.

SUPPORT FÖR FJÄRRSTYRDA ENHETER

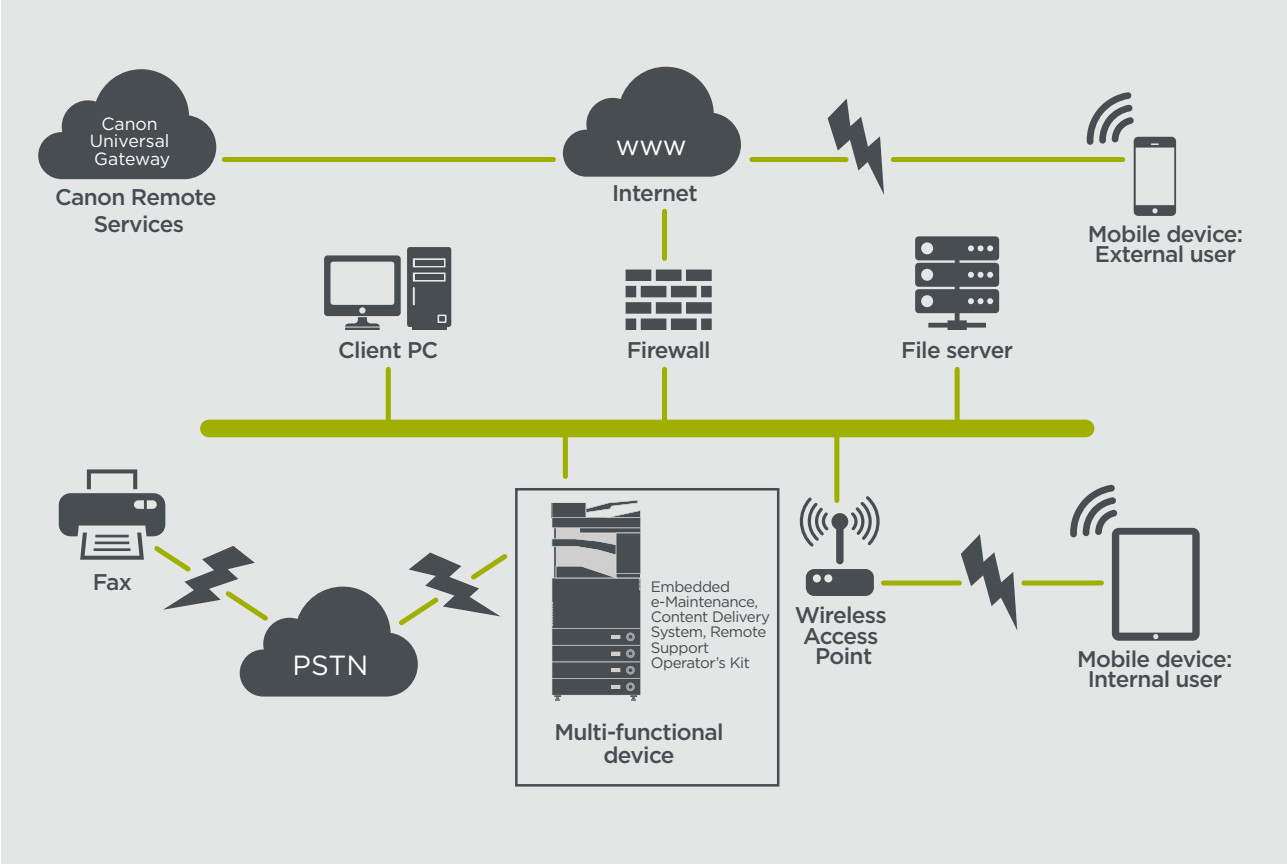
För att Canon eller en Canon-partner ska kunna tillhandahålla effektiv service kan imageRUNNER ADVANCE överföra servicerelaterade data och ta emot uppdateringar av den inbyggda programvaran eller programvaror. Vi vill uppmärksamma att inga bilder eller metadata för bilder skickas.

Nedan visas två möjliga implementeringar av Canons fjärrstyrda tjänster inom ett företags nätverk.

Implementeringsscenario 1: Spridd anslutning

Med den här inställning kan varje MFD ha direktanslutning till den fjärrstyrda tjänsten via internet.

Bild 9 Spridd anslutning



Implementeringsscenario 2: Centralt hanterad anslutning

I en miljö på ett stort företag där flera MFD:er är installerade är det nödvändigt att kunna hantera enheterna effektivt från en central punkt och det omfattar anslutningen till Canons fjärrstyrda tjänster. För att underlätta helhetssynen på hanteringen upprättar individuella enheter hanteringsanslutningar via en enda iWMC-anslutningspunkt (iW Management Console). För kommunikationen mellan plugin-programmet för uppdatering av enhetens inbyggda programvara (DFU) och multifunktionsenheter används UDP-porten 47545.

Bild 10 Centralt hanterad anslutning

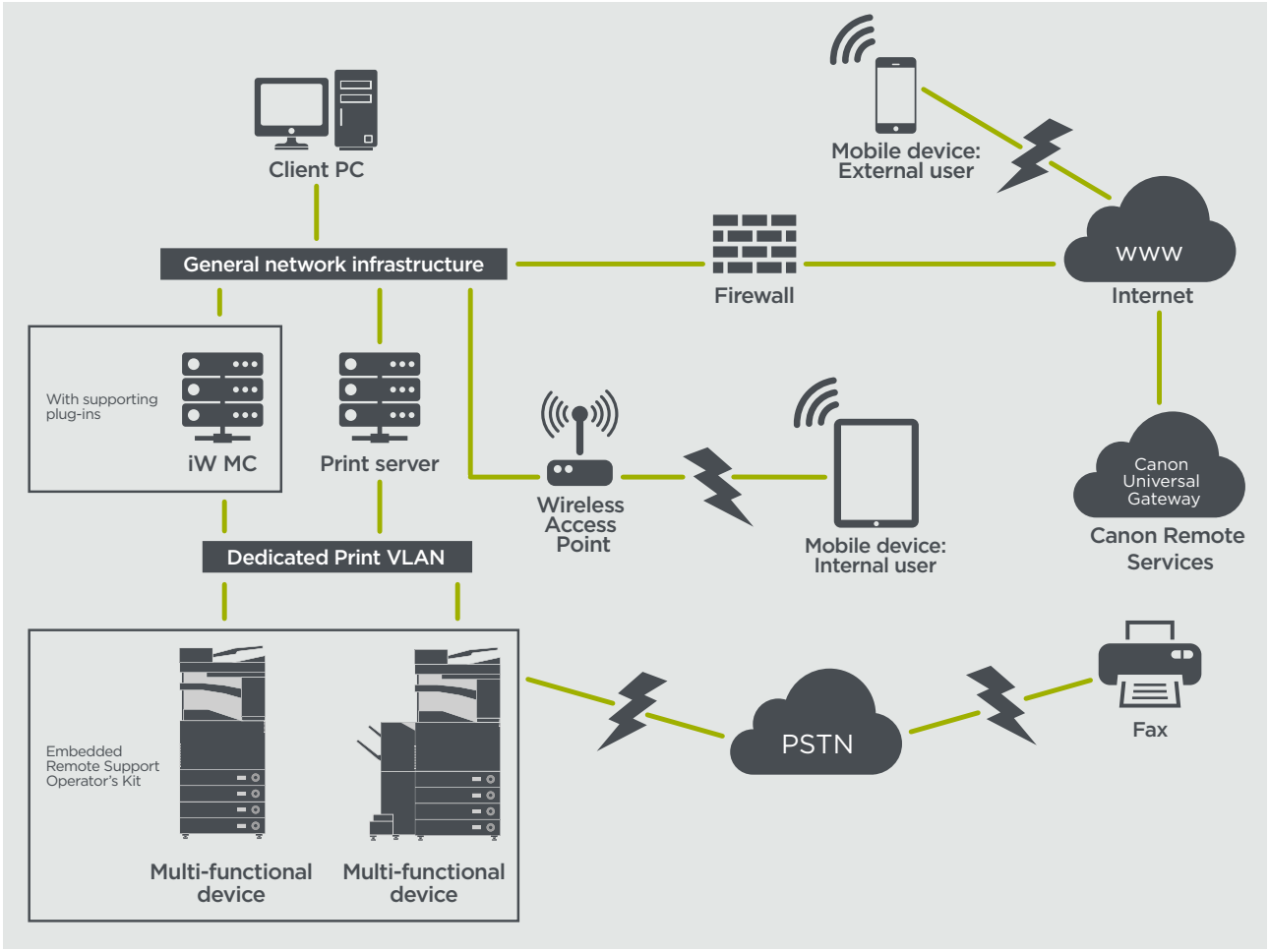


Bild
11a. Enhetslista (en enda enhet i det här fallet) enligt rapportering på imageWARE Management Console och
11b. Enhetsuppgifter och -inställningar

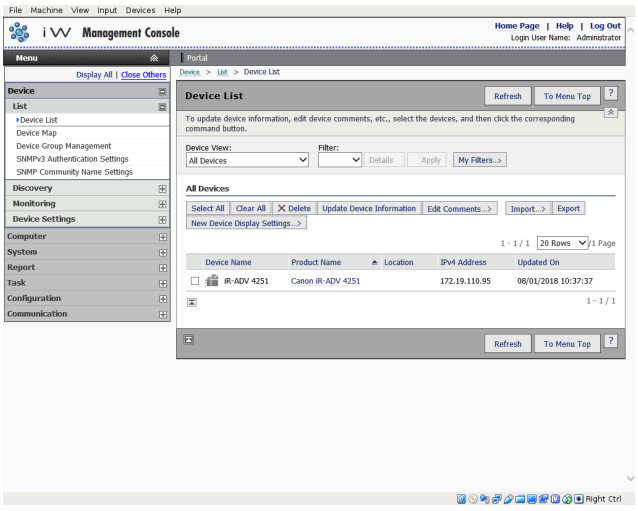


Bild 11a

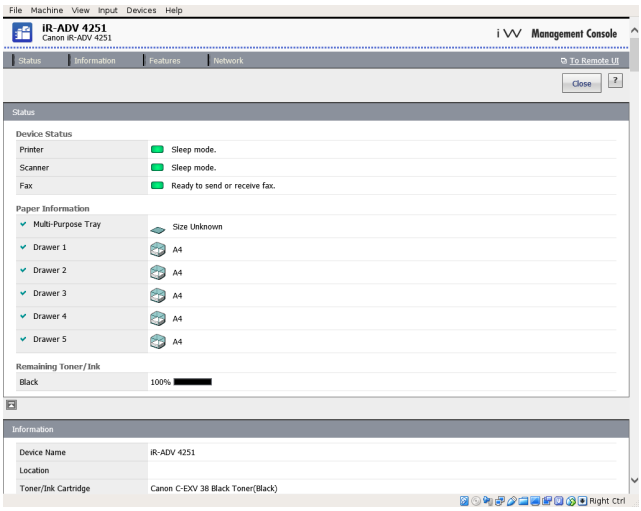


Bild 11b

e-Maintenance

e-Maintenance-systemet tillhandahåller ett automatiserat sätt för att samla in enhetsanvändningsräknare för faktureringsändamål, hantering av förbrukningsartiklar och övervakning av fjärrstyrda enheter via status- och felaviseringar.

e-Maintenance-systemet består av en server mot internet (UGW) och antingen en inbäddad programvara för multifunktionsenheter (eRDS) eller ytterligare serverbaserad programvara (plugin-programmet RDS) för att samla in information relaterad till enhetstjänster. eRDS är ett övervakningsprogram som körs i imageRUNNER ADVANCE. När övervakningsalternativet är aktiverat i enhetsinställningarna får eRDS sin egen enhetsinformation och skickar den till UGW. Plugin-programmet RDS är ett övervakningsprogram som installeras på en vanlig PC och kan övervaka 1–3 000 enheter. Det får information från varje enhet via nätverket och skickar det till UGW.

Som visas i tabell 4 nedan visas en översikt på nästa sida över överförda data, protokoll (beroende på vilka alternativ som väljs under utvecklingen och implementeringen) och portar som används. Bilddata för kopior, utskrifter, scanningar eller fax överförs aldrig.

Tabell 4 Dataöversikt för e-Maintenance

Beskrivning	Hanterade data	Protokoll/port	Port
Kommunikation mellan e-Maintenance (plugin-programmet eRDS eller RDS) och UGW	UGW-webbtjänstadress Proxyserveradress/portnummer Proxykonto/lösenord UGW-mejldestinationsadress SMTP-serveradress POP-serveradress Enhetsstatus, räknare och modellinformation Serienummer Information om återstående toner/bläck Information om inbyggd programvara Information om reparationsbegäran Information om loggning Servicesamtal Servicelarm Stopp Miljö Förhållandelogg	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Kommunikation mellan e-Maintenance och enhet (endast plugin-programmet RDS eftersom eRDS är inbäddad programvara)		SNMP Canons egna SLP/SLP/HTTPS	UDP/161 TCP/47546, UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Content Delivery System

CDS (Content Delivery System) upprättar en anslutning mellan MFD:en och UGW (Canon Universal Gateway). Den tillhandahåller uppdateringar av enhetens inbyggda programvara och program.

Tabell 5 Dataöversikt för Content Delivery System

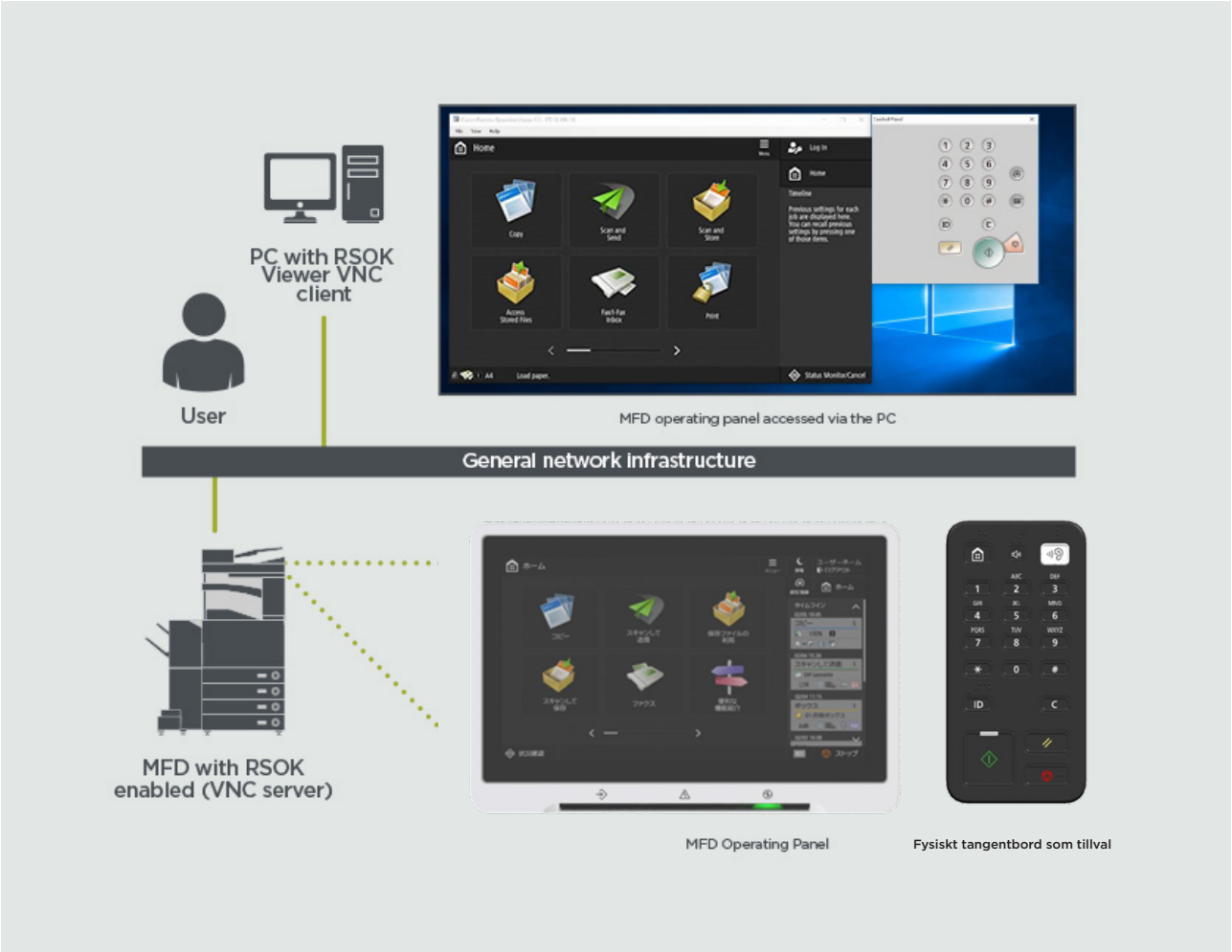
Beskrivning	Skickade data	Protokoll/port	Port
Kommunikation mellan MFD:n och UGW	Enhetens serienummer Version av inbyggd programvara Språk Land Information relaterad till enheten EULA	HTTP/HTTPS	TCP/80 TCP/443
Kommunikation mellan UGW och MFD:n	Testfil (binära slumpmässiga data) för kommunikationstester Binära data för inbyggd programvara eller MEAP-programvara	HTTP/HTTPS	TCP/80 TCP/443

Ett specifikt CDS med åtkomst till URL är förinställt i enhetskonfigurationen.
Om det finns ett krav på centraliserad hantering av enhetens inbyggda programvara och program inifrån infrastrukturen krävs en lokal installation av iWMC med plugin-programmen för uppdatering av enhetens inbyggda programvara (DFU) och hantering av enhetsprogram.

Fjärrsupport för användare

Fjärrsupport för användare (RSOK) ger fjärråtkomst till enhetens kontrollpanel. Det här server/klient-systemet består av en VNC-server som körs på MFP och klientprogrammet Remote Operation Viewer VNC Microsoft Windows.

Bild 12 Konfiguration av fjärrsupport för användare (RSOK)



Tabell 6 Dataöversikt för fjärrsupport för användare

Beskrivning	Skickade data	Protokoll/port	Port
VNC-lösenordsautentisering	Användarlösenord	Krypterad DES	5900
Operation Viewer	Enhetens kontrollpanel – skärmdata – maskinvarans knappfunktioner	Version 3.3 RFB-protokoll	5900

KÄLLOR

Säkerhetsrelaterade funktioner hos Canon imageRUNNER ADVANCE

imageRUNNER ADVANCE-plattformen ger fjärrstyrd konfiguration via ett webbtjänstgränssnitt som fjärranvändargränssnittet (RUI). Det här gränssnittet get åtkomst till flera av enhetens konfigurationsinställningar och kan avaktiveras om det inte är tillåtet och skyddas med lösenord för att förhindra obehörig åtkomst.

Även om majoriteten av enhetsinställningarna är tillgängliga via RUI är det nödvändigt att använda enhetens kontrollpanel för att ange alternativ som inte kan anges med det här gränssnittet. Vi rekommenderar att du avaktiverar alla tjänster som inte används och skärper kontrollerna för de som behövs. Fjärrsupport för användare (RSOK) ger fjärråtkomst till enhetens kontrollpanel för ökad flexibilitet och support. Det baseras på VNC-teknik som består av en server (MFD:n) och en klient (en nätverksdator). Det finns ett specifikt visningsprogram från Canon för klientdatorer som ger simulerad åtkomst till kontrollpanelens knappar vid behov.

Det här avsnittet ger en översikt över viktiga säkerhetsrelaterade funktioner hos imageRUNNER ADVANCE och deras konfigurationsinställningar.

Interaktiva användarhandböcker online finns på https://oip.manual.canon/ och innehåller information utöver säkerhetsrelaterade funktioner. Börja med att välja produkttypen (t.ex. imageRUNNER ADVANCE DX), klicka på sökikonen och ange dina sökvillkor. Nedan visas några allmänna områden som är värda att ha i åtanke.

Hantera maskinen

För att minska läckage av personuppgifter eller obehörig användning krävs ständiga och effektiva säkerhetsåtgärder. Genom att utse en administratör som hanterar enhetsinställningar kan användarhantering och säkerhetsinställningar begränsas till de som har behörighet.

Öppna länken nedan i en webbläsare och ange **administratörskonfiguration** i sökrutan. Då visas information relaterad till följande:

- Grundläggande hantering av enheten
- Begränsning av risker för försummelse, användarfel och missbruk
- Enhetshantering
- Hantering av systemkonfiguration och inställningar

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

IEEE P2600-standard

Flera imageRUNNER ADVANCE-modeller är kompatibla med IEEE P2600, en global standard för informationssäkerhet för multifunktionell kringutrustning och skrivare.

Länken nedan beskriver säkerhetskraven som definieras i IEEE 2600-standarden och hur enhetsfunktionerna uppfyller de kraven.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

IEEE 802.1X-autentisering

När det finns krav på att ansluta till ett 802.1X-nätverk måste enheten autentisera sig för att kontrollera att det är en behörig anslutning.

Öppna länken nedan i en webbläsare och ange **802.1X** i sökrutan.
https://oip.manual.canon/USRMA-4703-zz-CS-3700-enGB/

Tillämpa en säkerhetspolicy för maskinen

De senaste imageRUNNER ADVANCE-modellerna tillåter att säkerhetsinställningar för flera enheter, säkerhetspolicyn, hanteras i bunt via RUI. Ett separat lösenord kan användas för att tillåta att endast säkerhetsadministratören kan ändra inställningarna.

Öppna länken nedan i en webbläsare och ange **Tillämpa en säkerhetspolicy för maskinen** i sökrutan. Då visas information relaterad till följande:

- Använda ett lösenord för att skydda säkerhetspolicyinställningarna
- Konfigurera säkerhetspolicyinställningarna
- Alternativ för säkerhetspolicyinställningar

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

Hantera användare

Kunder som kräver högre säkerhet och effektivitet kan använda antingen de inbyggda funktionerna eller en utskriftshanteringslösning som uniFLOW.

Mer information om våra utskriftshanteringslösningar får du om du kontaktar våra lokala representanter eller läser produktbroschyren för uniFLOW.

Konfigurera nätverkets säkerhetsinställningar

Behöriga användare kan råka ut för oväntade förluster från attacker från skadliga tredje parter, till exempel att någon snokar i, förfalskar eller manipulerar data vid överföring via ett nätverk. Maskinen har stöd för flera funktioner som skyddar viktig och värdefull information från sådana attacker, för ökad säkerhet och sekretess.

Öppna länken nedan i en webbläsare och ange **Konfigurera nätverkets säkerhetsinställningar** i sökrutan. Då visas information relaterad till följande:

Länken nedan beskriver följande:

- Undvika obehörig åtkomst
- Ansluta till ett trådlöst LAN
- Konfigurera nätverksmiljön

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

Hantera hårddiskdata

Enhetens hårddisk används för att lagra enhetens operativsystem, konfigurationsinställningar och jobbinformation. De flesta enhetsmodellerna har fullständig kryptering av hårddisken (kompatibel med FIPS 140-2) som parar ihop den med den specifika enheten, vilket förhindrar att obehöriga användare läser den. Ett förberedande säkerhetschip till Canon MFP är certifierat som en kryptografisk modul under Cryptographic Module Validation Program (CMVP) som fastställts av USA och Kanada samt Japan Cryptographic Module Validation Program (JCMVP).

Öppna länken nedan i en webbläsare och ange **Hantera hårddiskdata** i sökrutan.

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

ÖVERSIKT ÖVER SÄKERHETSPOLICYINSTÄLLNINGAR

Tredje generationens imageRUNNER ADVANCE-modeller har säkerhetspolicyinställningar och användare för säkerhetsadministration. Det kräver att administratören lyckas logga in och, om det är konfigurerat, att ytterligare en säkerhetsadministratör loggar in med ytterligare ett lösenord.

Tabellen nedan visar tillgängliga inställningar.

1. Gränssnitt	Anmärkningar
Policy för trådlös anslutning	
Förbjud användning av direktanslutning	<Use Wi-Fi Direct> (använd Wi-Fi Direct) är inställt på <Off> (av) Det går inte att få åtkomst till maskinen från mobila enheter
Förbjud användning av trådlöst LAN	<Select Wired/Wireless LAN> (välj trådbundet/trådlöst LAN) är inställt på <Wired LAN> (trådbundet LAN) Det går inte att upprätta en trådlös anslutning med maskinen via en router eller åtkomstpunkt med trådlöst LAN
Policy för USB	
Förbjud användning som USB-enhet	<Use as USB Device> (användning som USB-enhet) är inställt på <Off> (av) Det går inte att använda funktionerna utskrift eller scanning från datorer som är anslutna via när användning som en USB-enhet är förbjuden
Förbjud använd som USB-lagringsenhet	<Use USB Storage Device> (använd USB-lagringsenhet) är inställt på <Off> (av) Det går inte att använda USB-lagringsenheter Däremot fungerar fortfarande servicefunktioner även om "Förbjud användning som USB-lagringsenhet" är ON (på) • Uppdatering av inbyggd programvara via USB-minne (från hämtningsläge) • Kopiera Sublog-data från enhet till USB (LOG2USB) • Kopiera rapporten från enhet till USB (RPT2USB)
Användningspolicy för nätverkskommunikation Obs! De här inställningarna gäller inte för kommunikation med IEEE 802.1X-nätverk, även om kryssrutan är markerad för [Always Verify Server Certificate When Using TLS/Verifiera alltid servercertifikat vid användning av TLS]	
Verifiera alltid signaturer för SMS/ WebDAV-serverfunktioner	I <SMB Server Settings> (SMB serverinställningar) är alternativen <Require SMB Signature for Connection> (kräv SMB-signatur för anslutning) och <Use SMB Authentication> (använd SMB-autentisering) inställda på <On> (på) och <Use TLS> (använd TLS) i <WebDAV Server Settings> (WebDAV serverinställningar) är inställt på <On> (på) När maskinen används som en SMB-server eller WebDAV-server verifieras digitala certifikatsignaturer under kommunikationen
Verifiera alltid servercertifikat vid användning av TLS	<Confirm TLS Certificate for WebDAV TX> (bekräfta TLS-certifikat för WebDAV TX), <Confirm TLS Certificate for SMTP TX> (bekräfta TLS-certifikat för SMTP TX), <Confirm TLS Certificate for POP RX> (bekräfta TLS-certifikat för POP RX), <Confirm TLS Certificate for Network Access> (bekräfta TLS-certifikat för nätverksåtkomst) och <Confirm TLS Certificate Using MEAP Application> (bekräfta TLS-certifikat med MEAP-programvara) är inställda på <On> (på) och en kryssmarkering läggs till i <CN> Dessutom är alternativen <Verify Server Certificate> (verifiera servercertifikat) och <Verify CN> (verifiera CN) i <SIP Settings> (SIP-inställningar) > <TLS Settings> (TLS-inställningar) inställda på <On> (på) Under TLS-kommunikationen utförs verifieringen för digitala certifikat och deras vanliga namn
Förbjud autentisering med klartext för serverfunktioner	• <Use FTP Printing> (använd FTP-utskrift) i <FTP Print Settings> (FTP-utskriftsinställningar) är inställt på <Off> (av) • <Allow TLS (SMTP RX)> (tillåt TLS (SMTP RX)) i <E-Mail/I-Fax Settings> (e-post-/I-Fax-inställningar) <Communication Settings> (kommunikationsinställningar) är inställt på <Always TLS> (alltid TLS), <Dedicated Port Authentication Method> (särskild autentiseringsmetod för port) i <Network> (nätverk) är inställt på <Mode 2> (läge 2), • <Use TLS> (använd TLS) i <WebDAV Server Settings> (WebDAV-serverinställningar) är inställt på <On> (på) När maskinen används som en server är funktioner som använder autentisering med vanlig text inte tillgängliga TLS används om autentisering med klartext är förbjuden. Det går inte att använda program eller serverfunktioner, till exempel FTP, som endast har stöd för autentisering med klartext Det kanske inte går att få åtkomst till maskinen från programvaran eller drivrutinen för enhetshantering
Förbjud användning av SNMPv1	I <SNMP Settings> (SNMP-inställningar) är <Use SNMPv1> (använd SNMPv1) inställt på <Off> (av) Du kanske inte kan hämta eller ange enhetsinformationen från skrivardrivrutinen eller hanteringsprogramvaran om användning av SNMPv1 är förbjuden
Policy för portanvändning	
Begränsa LPD-port	Portnummer: 515 <LPD Print Settings> (LPD-utskriftsinställningar) är inställt på <Off> (av) Det går inte att utföra LPD-utskrift
Begränsa RAW-port	Portnummer 9100 <LPD Print Settings> (RAW-utskriftsinställningar) är inställt på <Off> (av) Det går inte att utföra RAW-utskrift
Begränsa FTP-port	Portnummer 21 I <FTP Print Settings> (FTP-utskriftsinställningar är <Use FTP Printing> (använd FTP-utskrift) inställt på <Off> (av) Det går inte att utföra FTP-utskrift
Begränsa WSD-port	Portnummer 3702, 60000 I <WSD Settings> (WSD-inställningar) är alternativen <Use WSD> (använd WSD), <Use WSD Browsing> (använd WSD-bläddring) och <Use WSD Scan> (använd WSD-scanning) inställda på <Off> (av) Det går inte att använda WSD-funktioner

Begränsa BMLinkS-port	Portnummer 1900 Används inte i europeiska regioner
Begränsa IPP-port	Portnummer 631 Du kan inte använda Mopria, AirPrint och IPP om IPP-porten är begränsad
Begränsa SMB-port	Portnummer: 137, 138, 139, 445 I <SMB Server Settings> (SMB-serverinställningar) är <Use SMB Server> (använd SMB-server) inställt på <Off> (av) Det går inte att använda maskinen som en SMB-server
Begränsa SMTP-port	Portnummer 25 I <E-Mail/I-Fax Settings> (e-post-/I-Fax-inställningar) > <Communication Settings> (kommunikationsinställningar) är <SMTP RX> inställt på <Off> (av) SMTP-mottagning är inte möjlig
Begränsa särskild port	Portnummer: 9002, 9006, 9007, 9011–9015, 9017–9019, 9022, 9023, 9025, 20317, 47545–47547 Du kan inte använda fjärrfunktionerna för kopiera, faxa, scanna eller skriva ut, eller program, osv. när den särskilda porten är begränsad
Begränsa port för fjärranvändarens program	Portnummer 5900 <Remote Operation Settings> (inställningar för fjärranvändning) är inställt på <Off> (av) Det går inte att använda funktioner för fjärranvändning
Begränsa SIP-port (IP Fax)	Portnummer: 5004, 5005, 5060, 5061, 49152) <Use Intranet> (använd intranät) i <Intranet Settings> (intranätsinställningar), <Use NGN> (använd NGN) i <NGN Settings> (NGN-inställningar) och <Use VoIP Gateway> (använd VoIP-gateway) i <VoIP Gateway Settings> (inställningar för VoIP-gateway) är inställda på <Off> (av) Det går inte att använda IP Fax
Begränsa mDNS-port	Portnummer 5353 I <mDNS Settings> (mDNS-inställningar) är alternativen <Use IPv4 mDNS> (använd IPv4 mDNS) och <Use IPv6 mDNS> (använd IPv6 mDNS) inställda på <Off> (av) <Use Mopria> (använd Mopria) är inställt på <Off> (av) Det går inte att söka nätverket eller utföra automatiska inställningar med mDNS Det går inte heller att skriva ut med Mopria™ eller AirPrint
Begränsa SLP-port	Portnummer 427 I <Multicast Discovery Settings> (inställningar för Multicast-identifiering) är <Response> (svar) är inställt på <Off> (av) Det går inte att söka nätverket eller utföra automatiska inställningar vid användning av SLP
Begränsa SNMP-port	Portnummer 161 Du kanske inte kan hämta eller ange enhetsinformation från skrivardrivrutinen eller hanteringsprogramvaran när SNMP-porten är begränsad I <SNMP Settings> (SNMP-inställningar) är alternativen <Use SNMPv1> (använd SNMPv1) och <Use SNMPv3> (använd SNMPv3) inställda på <Off> (av)

2. Autentisering	Anmärkningar
Användningspolicy för autentisering	
Förbjud gästanvändare	• <Advanced Space Settings> (inställningar för avancerat utrymme) > <Authentication Management> (autentiseringshantering) är inställt på <On> (på) • <Login Screen Display Settings> (inställningar för inloggningsskärm) är inställt på <Display When Device Operation Starts> (visa när enheten startar) • <Restrict Job from Remote Device without User Auth> (begränsa jobb från fjärrenhet utan användarautentisering) är inställt på <On> (på) Oregistrerade användare kan inte logga in på maskinen Även utskriftsjobb som skickas från en dator avbryts
Tvinga inställning för automatisk utloggning	Den här inställningen loggar ut användaren från kontrollpanelen Den gäller inte för andra utloggningsmetoder (inställningsbart intervall på 10 sek–9 minuter) <Auto Reset Time> (tid för automatisk återställning) är aktiverat Användaren loggas automatisk ut om inga åtgärder utförs under en angiven tid Välj [Time Until Logout/Tid till utloggning] på fjärranvändargränssnittets inställningsskärmbild
Användningspolicy för lösenord	
Förbjud cachelagring av lösenord för externa servrar	Den här inställningen gäller inte för lösenord som användaren själv sparar, till exempel lösenord till adressböcker osv. <Prohibit Caching of Authentication Password> (förbjud cachelagring av autentiseringslösenord) är inställt på <On> (på) Användare måste alltid ange ett lösenord för att få åtkomst till en extern server
Visa varning när standardlösenord används	<Display Warning When Default Password Is in Use> (visa varning när standardlösenord används) är inställt på <On> (på) Ett varningsmeddelande visas när maskinens fabriksinställda standardlösenord används
Förbjud användning av standardlösenord för fjärråtkomst	<Allow Use of Default Password for Remote Access> (tillåt användning av standardlösenord för fjärråtkomst) är inställt på <Off> (av) Det går inte att använda det fabriksinställda standardlösenordet vid åtkomst till maskinen från en dator
Policy för lösenordsinställningar (policyn gäller inte för hantering av avdelnings-ID eller PIN-kod)	
Ange minsta antal tecken för lösenord	Minska antal tecken kan vara mellan 1 och 32
Ange lösenordets giltighetsperiod	Giltighetsperioden kan vara mellan 1 och 180 dagar
Förbjud användning av 3 eller fler identiska tecken efter varandra	
Tvinga användning av minst 1 versal	
Tvinga användning av minst 1 gemen	
Tvinga användning av minst 1 siffra	
Tvinga användning av minst 1 symbol	
Policy för utelåsning	
Aktivera utelåsning	Gäller inte för avdelnings-ID/PIN-kod till brevlåda, PIN-kod eller autentisering för säker utskrift osv. Tröskel för utelåsning: kan vara 1–10 gånger Tid för utelåsning: kan vara 1–60 minuter

3. Nyckel/certifikat	Anmärkningar
Förbjud användning av svag kryptering	Gäller för IPSec, TLS, Kerberos, S/MIME, SNMPv3 och trådlöst LAN Du kanske inte kan kommunicera med enheter som endast har stöd för svag kryptering
Förbjud användning av nyckel/certifikat med svag kryptering	Gäller för IPSec, TLS och S/MIME Om du använder en nyckel/certifikat med svag kryptering för TLS ändras den till den förinställda nyckeln/certifikatet. Du kan inte kommunicera om du använder en nyckel/certifikat med svag kryptering för andra funktioner än TLS
Använd TPM för att lagra lösenord och nyckel	Endast tillgängligt för enheter med TPM installerat. Säkerhetskopiera alltid TPM-nycklarna när TPM är aktiverat Mer information finns i användarhandboken Viktigt när TPM-inställningarna är aktiverade: • Se till att ändra lösenordet för "Administratör" från standardvärdet för att förhindra att tredje part kan säkerhetskopiera TPM-nyckeln. Om tredje part tar den säkerhetskopierade TPM-nyckeln kan du inte återställa TPM-nyckeln • För ökad säkerhet kan TPM-nyckeln endast säkerhetskopieras en gång. Om TPM-inställningarna är aktiverade är det viktigt att säkerhetskopiera TPM-nyckeln till ett USB-minne och lagra det på en säker plats för att undvika att det försvinner eller stjäls • Säkerhetsfunktionerna från TPM garanterar inte fullständigt skydd för data och maskinvara

4. Logg	Anmärkningar
Tvinga registrering av granskningslogg	• <Save Operation Log> (spara åtgärdslogg) är inställt på <On> (på) • <Display Job Log> (visa jobblogg) är inställt på <On> (på) • <Retrieve Job Log with Management Software> (hämta jobblogg med hanteringsprogramvara) i <Display Job Log> (visa jobblogg) är inställt på <Allow> (tillåt) • <Save Audit Log> (spara granskningslogg) är inställt på <On> (på) • <Retrieve Network Authentication Log> (hämta logg för nätverksautentisering) är inställt på <On> (på) Granskningsloggar registreras alltid när den här inställningen är aktiverad
Tvinga SNTP-inställningar	Ange SNTP-serveradress I <SNTP Settings> (SNTP-inställningar), <Use SNTP> (använd SNTP) är inställt på <On> (på) Tidsynkronisering via SNTP krävs Ange ett värde för [Server Name/Servernamn] på fjärranvändargränssnittets inställningsskärmbild
Rapportering om Syslog-logg	Aktivera Syslog-målinformation vid användning av en Syslog-server eller SIEM • <Username and password> (användarnamn och lösenord) • <SMB server name> (SMB-servernamn) • <Destination path> (målsökväg) • <Perform export time> (tid för export)

5. Jobb	Anmärkningar
Policy för utskrift	
Förbjud utskrift direkt av mottagna jobb	Mottagna jobb lagras i fax-/I-Fax-minnet om utskrift direkt av mottagna jobb är förbjudet • <Handle Files with Forwarding Errors> (hantera filer med vidarebefordringsfel) är inställt på <Off> (av) • <Use Fax Memory Lock> (använd lås på faxminne) är inställt på <On> (på) • <Use I-Fax Memory Lock> (använd lås på I-Fax-minne) är inställt på <On> (på) • <Memory Lock End Time> (sluttid för lås på minne) är inställt på <Off> (av) • <Display Print When Storing from Printer Driver> (visa utskrift vid lagring från skrivardrivrutin) i <Set/Register Confidential Fax Inboxes> (ställ in/registrera skyddade faxinkorgar) är inställt på <Off> (av) • <Settings for All Mail Boxes> (inställningar för alla brevlådor) > <Print When Storing from Printer Driver> (utskrift vid lagring från skrivardrivrutin) är inställt på <Off> (av) • <Box Security Settings> (säkerhetsinställningar för Box) > <Display Print When Storing from Printer Driver> (visa utskrift vid lagring från skrivardrivrutin) är inställt på <Off> (av) • <Prohibit Job from Unknown User> (förbjud jobb från okänd användare) är inställt på <On> (på) och <Forced Hold> (vänteläge) är inställt på <On> (på) Utskrift sker inte direkt, även när utskriftsåtgärder utförs
Policy för skicka/ta emot	
Tillåt endast sändning till registrerade adresser	I <Limit New Destination> (begränsa ny destination) är alternativen <Fax>, <E-Mail> (e-post), <I-Fax> och <File> (arkiv) inställda på <On> (på) Det går endast att skicka till destinationer som är registrerade i adressboken
Tvinga bekräftelse av faxnummer	Användare måste ange ett faxnummer igen som bekräftelse vid sändning av fax
Förbjud automatisk vidarebefordring	<Use Forwarding Settings> (inställningar för använd vidarebefordring) är inställt på <Off> (av) Det går inte att vidarebefordra fax automatiskt

6. Lagring	Anmärkningar
Tvinga fullständig borttagning av data	<Hard Disk Data Complete Deletion> (fullständig borttagning av hårddiskdata) är inställt på <On> (på)

Fullständiga tekniska data för imageRUNNER ADVANCE finns på webbplatsen
https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Svenska AB
169 88 Solna
Tel. +46 8 744 85 00
canon.se

Canon Inc.
Canon.com

Canon Europe
canon-europe.com

Swedish edition v1.0