MONITOIMILAITTEIDEN TIETOTURVAOPAS

imageRUNNER ADVANCE

Canon

JOHDANTO

Nykyaikaiset Canon-monitoimilaitteet (MFD) tarjoavat tulostus-, kopiointi-, skannaus-, lähetys- ja faksitoiminnot. Monitoimilaitteet ovat itsessään palvelimia, jotka tarjoavat erilaisia verkkopalveluja ja huomattavan määrän kiintolevytilaa.

Kun organisaatio liittää nämä laitteet infrastruktuuriinsa, on tarpeen huolehtia useista eri seikoista osana laajempaa tietoturvastrategiaa, jonka tarkoituksena on suojata verkkojärjestelmien luottamuksellisuutta, eheyttä ja saatavuutta.

Käyttöönotoissa on luonnollisesti eroja, ja organisaatioilla on omia tietoturvavaatimuksiaan. Teemme yhteistyötä sen varmistamiseksi, että toimitettavissa Canon-laitteissa on asianmukaiset suojauksen alkuasetukset, ja tarjoamme lisäksi määritysasetuksia, joiden avulla laitteen voi mukauttaa entistä paremmin tilanteeseen sopivaksi.

Tämä asiakirja on suunniteltu antamaan riittävästi tietoa, jotta pystyt keskustelemaan Canonin tai Canonin yhteistyökumppanin kanssa omaan käyttöympäristöösi parhaiten sopivista asetuksista. On hyvä muistaa, että kaikissa laitteistoissa ei ole samantasoisia ominaisuuksia ja että eri järjestelmien ohjelmistoissa saattaa olla erilaisia toimintoja. Kun lopullinen kokoonpano on päätetty, sitä voidaan käyttää laitteessa tai koko laitekannassa. Voit ottaa yhteyttä Canoniin tai Canon-kumppaniin, jos tarvitset lisätietoja tai tukea.

Kenelle tämä asiakirja on tarkoitettu?

Tämä asiakirja on tarkoitettu niille, jotka osallistuvat verkkoinfrastruktuurissa käytettävien toimiston monitoimilaitteiden suunnitteluun, käyttöönottoon ja suojaamiseen. Heitä voivat olla IT- ja verkkoasiantuntijat, tietoturva-asiantuntijat ja huoltohenkilöstö.

Kattavuus ja soveltamisala

Oppaassa kuvataan kahden tyypillisen verkkoympäristön määritysasetukset ja niiden käyttö, jotta organisaatiot voivat ottaa monitoimilaiteratkaisun käyttöön turvallisesti ja parhaiden käytäntöjen mukaisesti. Oppaassa kerrotaan myös, miten Syslog-toiminto voi antaa reaaliaikaista palautetta monitoimilaitteesta (järjestelmän ohjelmistoalustan versiosta 3.8 alkaen). Canonin tietoturvatiimi on testannut ja vahvistanut nämä asetukset.

Emme tee oletuksia tiettyjen alojen lainsäädännöllisistä vaatimuksista, joihin saattaa liittyä muita turvallisuusnäkökulmia, eikä niitä käsitellä tässä asiakirjassa.

Tämä opas laadittiin imageRUNNER ADVANCE -alustan tyypillisten ominaisuuksien pohjalta, ja vaikka tässä olevat tiedot pätevät kaikkiin imageRUNNER ADVANCE -valikoiman malleihin ja sarjoihin, jotkin ominaisuudet saattavat vaihdella mallien välillä.

Monitoimilaitteiden suojauksen käyttöönotto ympäristössä

Kun käsittelemme turvallisuusnäkökohtia, jotka liittyvät monitoimilaitteen käyttöönottoon osaksi verkkoa, käytämme kahta tyypillistä skenaariota:

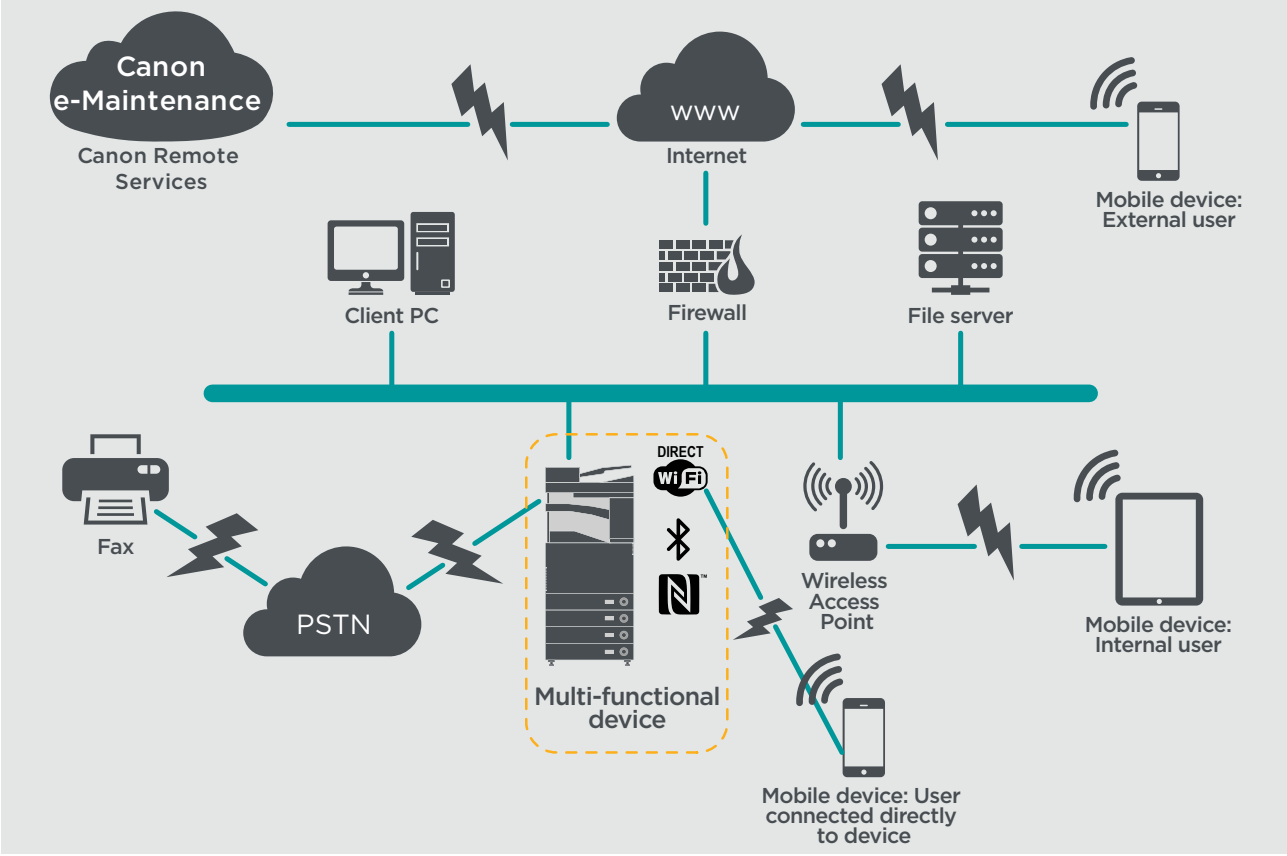
- **Tyypillinen pientoimistoympäristö**
- **Suuryrityksen toimistoympäristö**

PIENTOIMISTOYMPÄRISTÖ

Tämä on yleensä pienen yrityksen ympäristö, jonka verkkotopologiaa ei ole jaettu osiin. Siinä on sisäistä käyttöä varten yksi tai kaksi monitoimilaitetta, joita ei voi käyttää internetistä.

Vaikka mobiilitulostus on käytettävissä, muita ratkaisun komponentteja tarvitaan. Niillä käyttäjillä, jotka tarvitsevat tulostuspalveluja lähiverkkoympäristön ulkopuolella, on oltava suojattu yhteys, mutta sitä ei käsitellä tässä oppaassa. On kuitenkin otettava huomioon etälaitteen ja tulostusinfrastruktuurin välillä siirtyvien tietojen suojaus.

Kuva 1 Pientoimiston verkko



imageRUNNER ADVANCE -mallien uusimmassa sukupolvessa on langaton verkkoyhteys, jonka avulla laite voi muodostaa yhteyden Wi-Fi-verkkoon. Sen avulla voi muodostaa myös pisteiden välisen Wi-Fi Direct -yhteyden mobiililaitteella ilman verkkoyhteyttä.

Bluetooth- ja NFC-vaihtoehdot ovat saatavilla useissa laitemalleissa, ja niiden avulla voidaan muodostaa Wi-Fi Direct -yhteys vain iOS- ja Android-laitteille.

MÄÄRITYKSISSÄ HUOMIOITAVAA

Huomaa, että ellei imageRUNNER ADVANCE -laitteen ominaisuutta mainita alla, sen katsotaan riittävän oletusasetuksineen tässä yritys- ja verkkoympäristössä.

Taulukko 1 Pientoimistoympäristön määrityksissä huomioitavaa

imageRUNNER ADVANCE -ominaisuus	Kuvaus	Huomioitavaa
Huoltotila	Tarjoaa pääsyn Huoltotilan asetuksiin	Suojaa salasanalla, joka on muu kuin oletussalasana, riittävän monimutkainen ja enimmäispituuden mukainen.
Service Management System (Huollon hallintajärjestelmä)	Tarjoaa pääsyn erilaisiin vakioasetuksista poikkeaviin laiteasetuksiin	Suojaa salasanalla, joka on muu kuin oletussalasana, riittävän monimutkainen ja enimmäispituuden mukainen.
SMB-selaus/-lähetys	Tallenna ja nouda käyttämällä Windows-/SMB-verkkoasemia	Järjestelmänvalvojien on estettävä käytäntöjen avulla käyttäjiä luomasta paikallisia tilejä asiakaslaitteisiinsa asiakirjojen jakamiseen imageRUNNER ADVANCE -laitteella ja SMB-yhteydellä.
Etäkäyttöliittymä	Verkkopohjainen määritystyökalu	imageRUNNER ADVANCE -järjestelmänvalvojan on otettava HTTPS käyttöön etäkäyttöliittymää varten ja poistettava HTTP käytöstä. Ota käyttöön kunkin laitteen yksilöllisen PIN-todennuksen käyttö.
SNMP	Verkonvalvonnan integrointi	Poista versio 1 käytöstä ja ota käyttöön ainoastaan versio 3.
Lähetä sähköpostiin ja/tai IFAX-palveluun	Liitteitä sisältävien sähköpostien lähetys laitteelta	Ota SSL käyttöön. Älä käytä POP3-todennusta ennen SMTP-lähetystä. Käytä SMTP-todennusta.
POP3	Hae ja tulosta asiakirjoja automaattisesti postilaatikosta	Ota SSL käyttöön. Ota POP3-todennus käyttöön.
Osoitekirja/LDAP	Käytä hakemistopalvelua kotinumeron tai sähköpostiosoitteiden hakemiseen skannausten lähettämistä varten.	Ota SSL käyttöön. Älä käytä toimialueen tunnistetietoja LDAP-palvelinta käyttävässä todennuksessa, vaan käytä LDAP-kohtaisia tunnistetietoja.
FTP-tulostus	Lähetä ja lataa asiakirjoja käyttämällä sisäistä FTP-palvelinta	Ota FTP-todennus käyttöön. Huomaa, että FTP-liikenne kulkee aina selväkielisenä tekstinä verkossa
WebDAV-lähetys	Skannaa ja tallenna asiakirjoja etäsijaintiin	Ota todennus käyttöön WebDAV-verkkoasemissa.
Salattu PDF	Salaa asiakirjat	Käytäntöjen mukaan arkaluonteiset asiakirjat tulee salata vain käyttämällä PDF-versiota 1.6 (AES-128).
Turvatulostus	Tulostustyö lähetetään laitteeseen, mutta lukitaan tulostusjonoon, kunnes vastaava PIN-koodi annetaan	Ota PIN-koodilla suojatut tulostustyöt käyttöön.
Syslog-tapahtumailmoitus	System Logging Protocol on alan vakioprotokolla, jolla lähetetään järjestelmäloki- tai tapahtumaviestejä Syslog-palvelimeen	Voit kohdistaa imageRUNNER -laitteen Syslog-tiedot olemassa olevaan verkon järjestelmälokien analyysityökaluun tai yrityksen SIEM (Security Event Management System) -järjestelmään.
Suojattu käynnistys (käynnistyksen yhteydessä tehtävä tarkistus)	Antaa varmistuksen siitä, että järjestelmän ohjelmistokomponentit eivät ole vaarantuneet. Tällä on vähäinen vaikutus järjestelmän käynnistysaikaan.	Ota toiminto käyttöön.
Sisäinen verkkoselain	Pääsy selaimella internetiin	Pakota hallinnan avulla sisältöä suodattavan verkon välityspalvelimen käyttö, jotta vältetään haitallisen tai viruksia sisältävän sisällön käyttö. Poista suosikkien luonti käytöstä.
Bluetooth ja NFC (saatavilla Generation 3 -malleista alkaen)	Käytetään Wi-Fi Direct -yhteyden luomiseen	Ottamalla Wi-Fi Directin käyttöön sallit suoran yhteyden mobiililaitteeseen. Wi-Fi Directiä ei voi käyttää, kun Wi-Fi-yhteydellä muodostetaan yhteys verkkoon.
Langaton lähiverkko	Tarjoaa langattoman käytön	Käytä WPA-PSK-/WPA2-PSK-suojausta ja vahvoja salasanoja.
IPP	Luo yhteys ja lähetä tulostustöitä IP-yhteydellä	Poista IPP käytöstä.

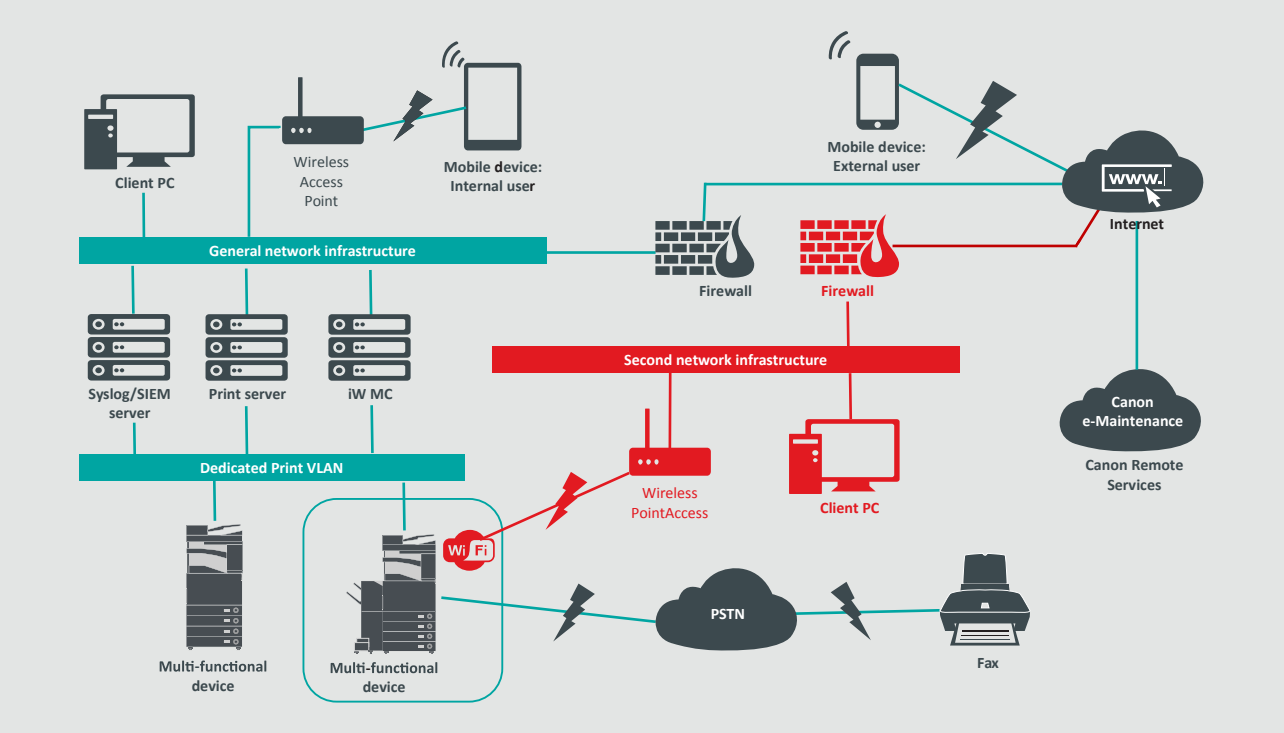
SUURYRITYKSEN TOIMISTOYMPÄRISTÖ

Tämä on yleensä useita toimipaikkoja ja toimistoja kattava ympäristö, jonka verkkoarkkitehtuuri on jaettu segmentteihin. Siinä on useita erillisessä virtuaalilähiverkossa olevia monitoimilaitteita, joita voi käyttää sisäisesti tulostuspalvelinten kautta. Näitä monitoimilaitteita ei voi käyttää internetistä.

Tällaisessa ympäristössä on yleensä pysyvä tiimi verkko- ja taustatoimintojen vaatimusten ja yleisten tietokoneongelmien tukea varten, mutta tiimeillä ei odoteta olevan monitoimilaitteiden koulutusta.

Tämä on yleensä useita toimipaikkoja ja toimistoja kattava ympäristö, jonka verkkoarkkitehtuuri on jaettu segmentteihin. Siinä on useita erillisessä virtuaalilähiverkossa olevia monitoimilaitteita, joita voi käyttää sisäisesti tulostuspalvelinten kautta. Näitä monitoimilaitteita ei voi käyttää internetistä.

Kuva 2 Suuryrityksen toimistoverkko



Punaisella korostetut yhteydet ovat saatavilla Generation 3 -malleista alkaen

MÄÄRITYKSISSÄ HUOMIOITAVAA

Huomaa, että ellei imageRUNNER ADVANCE -laitteen toimintoa mainita alla, sen katsotaan riittävän oletusasetuksineen tässä yritys- ja verkkoympäristössä.

Taulukko 2 Suuryrityksen toimistoympäristön määrityksissä huomioitavaa

imageRUNNER ADVANCE -ominaisuus	Kuvaus	Huomioitavaa
Huoltotila	Tarjoaa pääsyn huoltotilan asetuksiin	Suojaa salasanalla, joka on muu kuin oletussalasana, riittävän monimutkainen ja enimmäispituuden mukainen.
Service Management System (Huollon hallintajärjestelmä)	Tarjoaa pääsyn erilaisiin vakioasetuksista poikkeaviin laiteasetuksiin	Suojaa salasanalla, joka on muu kuin oletussalasana, riittävän monimutkainen ja enimmäispituuden mukainen.
SMB-selaus/-lähetys	Tallenna ja nouda käyttämällä Windows-/SMB-verkkoasemia	Järjestelmänvalvojien on estettävä käytäntöjen avulla käyttäjiä luomasta paikallisia tilejä laitteisiinsa asiakirjojen jakamiseen imageRUNNER ADVANCE -laitteella ja SMB-yhteydellä.
Etäkäyttöliittymä	Verkkopohjainen määritystyökalu	Käytä laitteen alkuperäisiä asetuksia ja poista etäkäyttöliittymä kokonaan käytöstä poistamalla HTTP ja HTTPS käytöstä.
SNMP	Verkonvalvonnan integrointi	Poista versio 1 käytöstä ja ota käyttöön ainoastaan versio 3.
Lähetä sähköpostiin ja/tai IFAX-palveluun	Liitteitä sisältävien sähköpostien lähetys laitteelta	Ota SSL käyttöön. Käytössä: - Varmenteen vahvistus SMTP-palvelimessa Jos tämä ei käy: - Käytä tätä toimintoa vain ympäristössä, jossa on verkkoon tunkeutumisen havaitsemisjärjestelmä. Älä käytä POP3-todennusta ennen SMTP-lähetystä. Käytä SMTP-todennusta.
POP3	Hae ja tulosta asiakirjoja automaattisesti postilaatikosta	Ota SSL käyttöön. Käytössä: - Varmenteen vahvistus POP3-palvelimessa Jos tämä ei käy: - Käytä tätä toimintoa vain ympäristössä, jossa on verkon tunkeutumisenhavaitsemisjärjestelmän keruutyökalu. Ota POP3-todennus käyttöön.
Osoitekirja/LDAP	Käytä hakemistopalvelua puhelinnumeron tai sähköpostiosoitteiden hakemiseen skannausten lähettämistä varten	Ota SSL käyttöön. Käytössä: - Varmenteen vahvistus LDAP-palvelimessa Jos tämä ei käy: - Käytä tätä toimintoa vain ympäristössä, jossa on verkkoon tunkeutumisen havaitsemisjärjestelmä. Älä käytä toimialueen tunnistetietoja LDAP-palvelinta käyttävässä todennuksessa, vaan käytä LDAP-kohtaisia tunnistetietoja.
IPP	Luo yhteys ja lähetä tulostustöitä IP-yhteydellä	Poista IPP käytöstä.
WebDAV-lähetys	Skannaa ja tallenna asiakirjoja etäsijaintiin	Ota todennus käyttöön WebDAV-verkkoasemissa. Ota SSL käyttöön. Pakota tulostin sallimaan vain sellaisten tiedostojen lataaminen, joissa on tulostuksen tiedostotunnisteet.
IEEE802.1X	Verkon käytön todennusmekanismi	EAPOL V1 on tuettu.
Salattu PDF	Salaa asiakirjat	Käytäntöjen mukaan arkaluonteiset asiakirjat saa salata vain PDF-versiolla 1.6 (AES-128).
Salattu tietoturvallinen tulostus	Paranna turvatulostuksen suojausta salaamalla tiedosto ja salasana siirron aikana	Määritä työaseman tulostinmääritysten tulostinvälilehdessä käyttäjänimeksi muu käyttäjänimi kuin käyttäjän LDAP-/toimialueen tunnistetiedot. Varmista, että "Restrict printer jobs/Rajoita tulostustöitä" on poistettu käytöstä.
Varmenteiden automaattinen rekisteröinti	Automaattinen rekisteröintiprosessi tehostaa digitaalisten varmenteiden noutoa ja käyttöönottoa	Vaatii verkkopohjaisen varmenneratkaisun käyttöä varten.
Syslog-tapahtumailmoitus	System Logging Protocol on alan vakioprotokolla, jolla lähetetään järjestelmäloki- tai tapahtumaviestejä Syslog-palvelimeen	Voit kohdistaa imageRUNNER ADVANCE -laitteen Syslog-tiedot olemassa olevaan verkon järjestelmälokien analyysityökaluun tai yrityksen SIEM (Security Event Management System) -järjestelmään.
Suojattu käynnistys (järjestelmän käynnistyksen yhteydessä tehtävä tarkistus)	Antaa varmistuksen siitä, että järjestelmän ohjelmistokomponentit eivät ole vaarantuneet. Tällä on vähäinen vaikutus järjestelmän käynnistysaikaan.	Ota toiminto käyttöön.
Langaton lähiverkko	Tarjoaa langattoman käytön	Käytä WPA-PSK-/WPA2-PSK-suojausta ja vahvoja salasanoja.
Wi-Fi Direct	Käytetään Wi-Fi Direct -yhteyden luomiseen	Poista Wi-Fi Direct käytöstä.
Sisäinen verkkoselain (saatavilla Generation 3 -laitteiden 2nd Edition -malleista alkaen)	Pääsy selaimella internetiin	Määritä asianmukaiset rajoitukset tai poista käytöstä mahdollisuus ladata selaimen kautta saatavia tiedostoja.

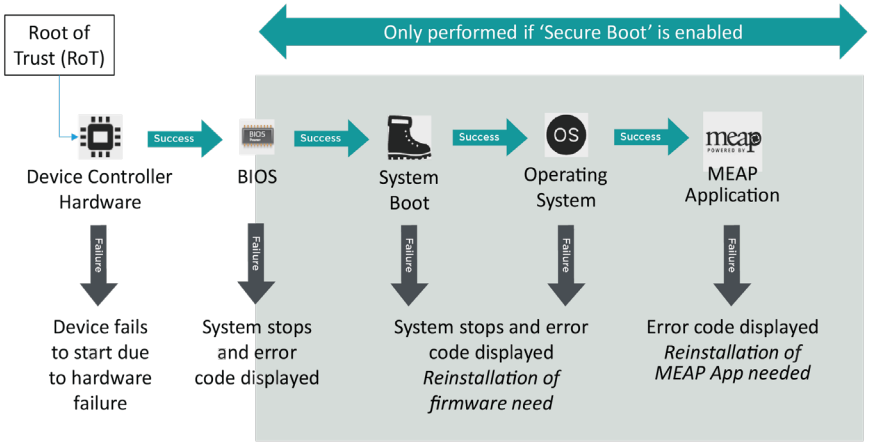
imageRUNNER ADVANCE -mallien uusimmassa sukupolvessa on langaton verkkoyhteys, jonka avulla laite voi muodostaa yhteyden Wi-Fi-verkkoon samaan aikaan kun sillä on yhteys kiinteään verkkoon. Tämä skenaario voi olla hyödyllinen, kun asiakkaan on jaettava laite kahden verkon välillä. Koulu on tyypillinen esimerkki ympäristöstä, jossa on eri verkko henkilökunnalle ja oppilaille.

imageRUNNER ADVANCE -alusta tarjoaa toiminnot joustavaa käyttöä varten. Koska tarvittavat protokollat ja palvelut ovat saatavilla, on tärkeää varmistaa, että vain käyttäjän tarpeiden täyttämiseen vaaditut toiminnot, palvelut ja protokollat otetaan käyttöön. Tämä on hyvä tietoturvakäytäntö, joka pienentää mahdollista hyökkäyspintaa ja estää sen hyväksikäytön. Koska uusia haavoittuvuuksia ilmenee jatkuvasti, on tärkeää olla varuillaan, jotta laitetta ei vaaranneta sisäisesti tai ulkoisesti. Mahdollisuus valvoa käyttäjien toimintaa auttaa tunnistamaan ongelmat ja suorittamaan korjaavia toimia tarpeen mukaan.

imageRUNNER ADVANCE -ohjelmistoalustan versioon 3.8 on lisätty joitakin toimintoja niiden lisäksi, jotka ovat olleet saatavilla jo vuosien ajan. Niihin kuuluu mahdollisuus valvoa laitetta reaaliaikaisesti Syslogin ja järjestelmän käynnistyksen yhteydessä tehtävän tarkistuksen avulla. Kun näitä toimintoja käytetään yhdessä olemassa olevien verkkoturvallisuusratkaisujen kanssa, esimerkiksi SIEM (Security Information and Event Management) -järjestelmien tai kirjausratkaisujen kanssa, saadaan laajempi näkyvyys ja voidaan tunnistaa häiriöt myös teknisiä analyyseja varten.

Suojattu käynnistys (Järjestelmän käynnistyksen yhteydessä tehtävä tarkistus)

Tämä toiminto on laitteiston mekanismi, joka on suunniteltu varmistamaan, että kaikki imageRUNNER ADVANCE Generation 3 3rd edition -järjestelmän osat tarkistetaan Root of Trust -toiminnolla sen takaamiseksi, että käyttöjärjestelmä latautuu Canonin tarkoittamalla tavalla. Jos hyökkääjä yrittää peukaloida tai muokata järjestelmää tai jos järjestelmän lataamisessa ilmenee virhe, prosessi pysähtyy ja näkyviin tulee virhekoodi.



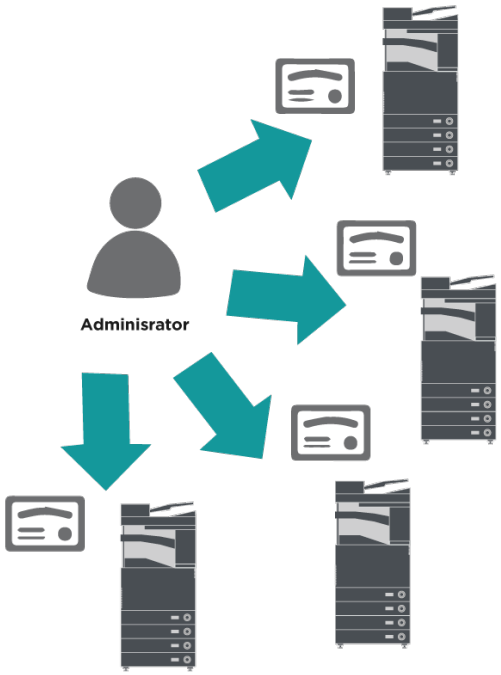
Kuva 3 Järjestelmän käynnistyksen yhteydessä tehtävä tarkistus

Prosessi ei näy käyttäjälle lukuun ottamatta näytöllä näkyvää ilmoitusta virheellisen järjestelmäversion lataamisesta. imageRUNNER ADVANCE Generation 3 3rd edition ja DX -laitteissa voi ottaa käyttöön järjestelmän käynnistyksen yhteydessä tehtävän tarkistuksen, jonka avulla tämä suojaustoiminto otetaan käyttöön.

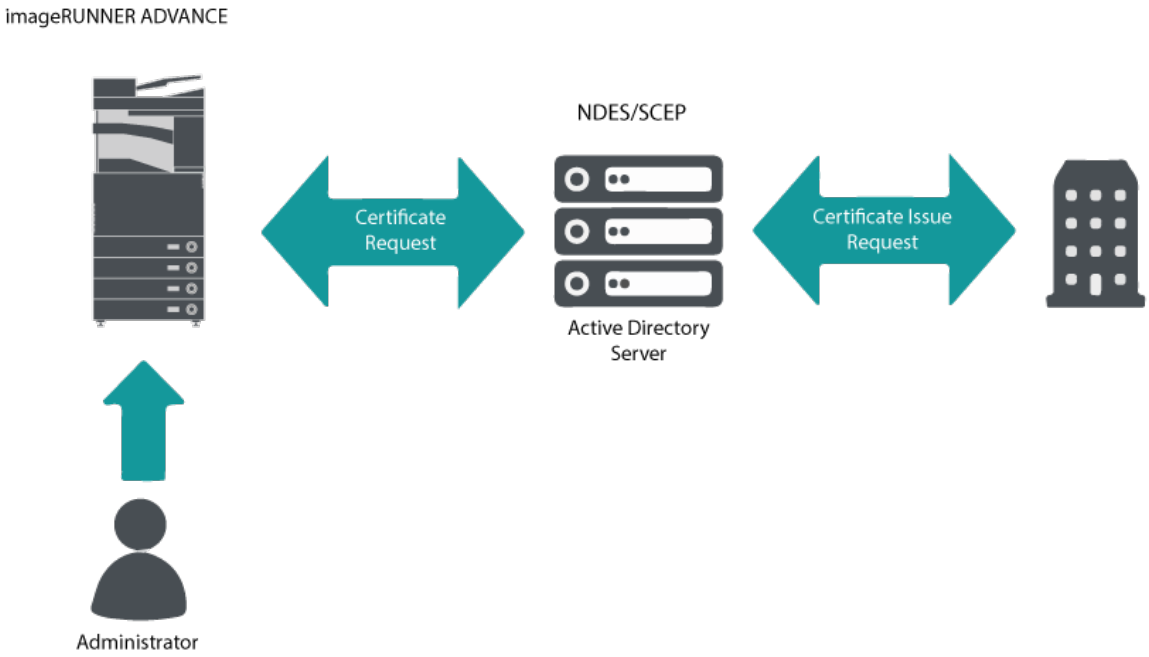
Varmenteiden automaattinen rekisteröinti

imageRUNNER ADVANCE -järjestelmän ohjelmistoalustan versiota 3.8 edeltävissä versioissa järjestelmänvalvojan oli asennettava päivitetyt suojausvarmenteet käsin kuhunkin laitteeseen.
Tämä vaati paljon työtä, koska jokainen laite oli yhdistettävä vuorotellen manuaalista päivitystä varten, ja varmenteet oli asennettava kunkin laitteen etäkäyttöliittymällä (RUI), mikä vei vielä enemmän aikaa. Koska varmenteiden automaattinen rekisteröintipalvelu on ollut käytössä alustan versiosta 3.8 alkaen, nämä kustannukset ovat poistuneet.

Automaattinen rekisteröintiprosessi tehostaa varmenteiden noutoa. Se antaa mahdollisuuden noutaa varmenteet automaattisesti käyttämällä Microsoft Windowsin verkkolaitteen rekisteröintipalvelua (NDES) ja Simple Certificate Enrollment Protocol (SCEP) -protokollaa.



Kuva 4 Varmenteen rekisteröinti



Kuva 5 Varmenteen rekisteröintiprosessi

SCEP on protokolla, joka tukee varmenteen myöntäjän (CA) myöntämiä varmenteita, ja NDES-palvelulla verkkolaitteet voivat noutaa tai ladata varmenteita SCEP:n avulla.

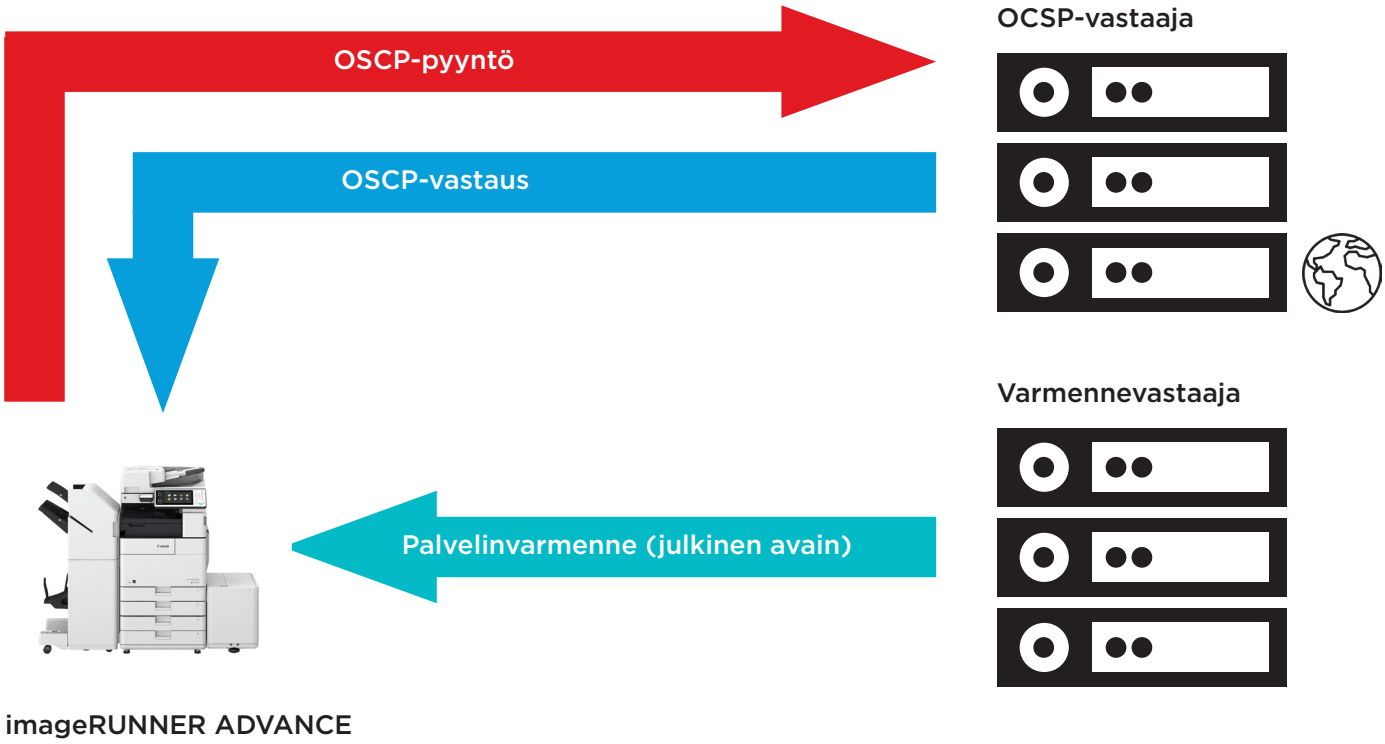
NDES on Active Directory -varmennepalveluiden roolipalvelu.

Online Certificate Status Protocol

On joitakin syitä, joiden takia digitaalisen varmenteen kumoaminen voi olla tarpeen. Yksityinen avain on saattanut kadota tai vaarantua tai se on voitu varastaa, tai toimialueen nimeä on saatettu muuttaa.

Online Certificate Status Protocol (OCSP) on Internetin vakioprotokolla, jolla tarkistetaan varmennepalvelimen myöntämien digitaalisten X.509-varmenteiden kumoamistila. Kun OCSP-vastaajalle (yleensä varmenteen myöntäjälle) lähetetään OCSP-pyyntö ja määritetään tietty varmenne, OCSP-vastaaja vastaa ilmoittamalla tilan ”hyvä”, ”kumottu” tai ”tuntematon”.

Kuva 6 OCSP:n kättelyprosessi



OCSP tarjoaa imageRUNNER ADVANCE -laitteiden alustan versiosta 3.10 alkaen reaaliaikaisen mekanismin asennettujen digitaalisten X.509-varmenteiden vahvistamiseen. Alustan aiemmat versiot tukivat vain varmenteiden sulkulistan (CRL) käyttöä, mutta mekanismi on tehoton ja kuluttaa paljon verkkoresursseja.

Suojaustiedot ja tapahtumien hallinta

imageRUNNER ADVANCE -teknologia tukee reaaliaikaisten tietoturvatapahtumien lähettämistä Syslog-protokollalla asiakirjojen RFC 5424, RFC 5425 ja RFC 5426 mukaisesti.

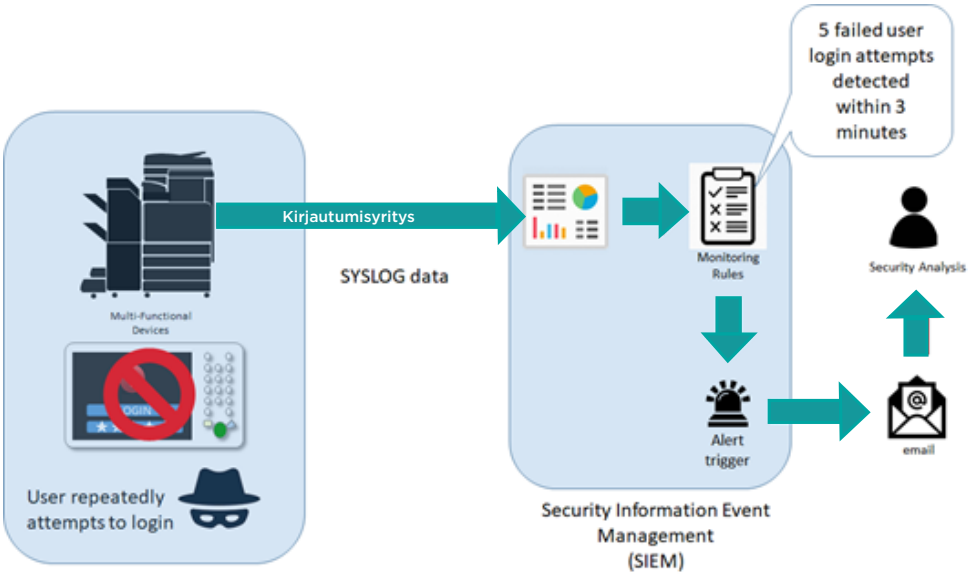
Monet laitetyypit käyttävät tätä protokollaa sellaisten reaaliaikaisten tietojen keräämiseen, joita voidaan käyttää mahdollisten tietoturvaongelmien tunnistamiseen.

Jotta uhkien ja tietoturvaongelmien havaitseminen on helpompaa, laite on määritettävä osoittamaan kolmannen osapuolen SIEM (Security Incident Event Management) -palvelimeen.

Laitteen tuottamia Syslog-tapahtumia voi käyttää toimien käynnistämiseen useiden tilannetietoja sisältävien tietolähteiden tapahtumien reaaliaikaisen keräämisen ja analysoinnin avulla (kuva 7). Tämä voi myös tukea vaatimustenmukaisuuden raportointia ja häiriöiden tutkimista, kun käytössä on lisäratkaisuja, kuten SIEM-palvelin. Kuvassa 8 on esimerkki tästä.

imageRUNNER ADVANCE -laitteiden uusimmassa sukupolvessa on Syslog-toiminto, joka tukee monenlaisten tapahtumien keräämistä. Tämän avulla voidaan verrata ja analysoida useiden erillisten lähteiden tapahtumia ja löytää trendejä tai poikkeavuuksia.

Kuva 7 Syslog-tietojen tallennus



Kuva 8 Esimerkki imageRUNNER ADVANCE -laitteen Syslog-tietojen käytöstä

Laitteen lokien hallinta

Järjestelmän ohjelmistoalustan versiosta 3.8 alkaen tarjotun Syslog-toiminnon lisäksi imageRUNNER ADVANCE tuottaa seuraavat lokit, joita voi hallita laitteessa. Nämä lokit voi viedä CSV-tiedostomuotoon etäkäyttöliittymässä (RUI).

Taulukko 3 – Esimerkkejä lokitiedostoista, joita voi hallita monitoimilaitteella

Lokityyppi	Lokityypin numero CSV-tiedostossa	Kuvaus
Loki	4098	Tässä lokissa on tietoja, jotka liittyvät käyttäjätodennuksen todennuksen tilaan (sisäänkirjautuminen/uloskirjautuminen ja käyttäjän todennuksen onnistuminen/epäonnistuminen), käyttäjän todennuksella hallittujen käyttäjän tietojen rekisteröimiseen/muuttamiseen/poistamiseen ja roolien hallintaan (lisääminen/muokkaaminen/poistaminen) KÄYTÖNHALLINTAJÄRJESTELMÄLLÄ.
Työloki	1001	Tässä lokissa on tietoja kopiointi-, faksaus-, skannaus-, lähetys- ja tulostustöiden valmistumisesta.
Siirtoloki	8193	Tässä lokissa on tietoja tiedonsiirroista
Advanced Space -tallennusloki	8196	Tässä lokissa on tietoja tiedostojen tallentamisesta Advanced Space -tallennustilaan, verkkoon (muiden laitteiden Advanced Space -tallennustilaan) ja muistivälineisiin.
Postilaatikon toimintoloki	8197	Tässä lokissa on tietoja toiminnoista, joita on suoritettu tiedoille postilaatikossa, muistin vastaanoton Saapuneet-kansiossa ja luottamuksellisten faksien Saapuneet kansiossa.
Postilaatikon todennusloki	8199	Tässä lokissa on tietoja postilaatikon, muistin vastaanoton Saapuneet-kansion ja luottamuksellisten faksien Saapuneet kansion todennuksen tilasta.
Advanced Space -toimintoloki	8201	Tässä lokissa on tietoja toiminnoista, joita on suoritettu tiedoille Advanced Space -tallennustilassa.
Laitteen hallintaloki	8198	Tässä lokissa on tietoja, jotka liittyvät laitteen käynnistämiseen/sammuttamiseen, asetuksiin Settings/Registration-näytössä tehtyihin muutoksiin, asetuksiin Device Information Delivery -toiminnolla tehtyihin muutoksiin sekä aika-asetukseen. Laitteen hallintaloki tallentaa myös käyttäjätietojen tai tietoturvaan liittyvien asetusten muutokset, kun paikallinen valtuutettu Canon-jälleenmyyjä tutkii tai korjaa laitteen.
Verkon todennusloki	8200	Tämä loki tallennetaan, kun IPSec-tietoliikenne epäonnistuu.
Vie/tuo kaikki -loki	8202	Tässä lokissa on tietoja asetusten tuonnista/viennistä Vie kaikki / Tuo kaikki -toiminnolla.
Postilaatikon varmuuskopiointiloki	8203	Tässä lokissa on tietoja, jotka liittyvät tietojen varmuuskopioihin käyttäjien Saapuneet-kansioissa, muistin vastaanoton Saapuneet-kansiossa, luottamuksellisten faksien Saapuneet kansiossa ja Advanced Space -tallennustilassa ja muihin säilytettyihin tietoihin sekä Päällekkäiskuva-toiminnolle rekisteröityyn lomakkeeseen.
Sovelluksen/ohjelmiston hallintanäytön toimintoloki	3101	Tämä on toimintoloki, joka liittyy SMS (Service Management Service) -palveluun, ohjelmiston rekisteröinteihin/päivityksiin, MEAP-sovellusten asennusohjelmiin jne.
Turvallisuuskäytännön loki	8204	Tässä lokissa on tietoja turvallisuuskäytännön asetusten tilasta.
Ryhmän hallintaloki	8205	Tässä lokissa on tietoja, jotka liittyvät käyttäjäryhmien asetusten tilaan (rekisteröimiseen/muokkaamiseen/poistamiseen).
Järjestelmän ylläpitoloki	8206	Tässä lokissa on tietoja laiteohjelmiston päivityksistä ja MEAP-sovelluksen varmuuskopioinnista/palautuksesta jne.
Valtuutetun tulostuksen loki	8207	Tässä lokissa on pakotettu pito -tulostustöiden tietoja ja toimintohistoria.
Asetusten synkronointiloki	8208	Tässä lokissa on tietoja laitteen asetusten synkronoinnista. Useiden Canonin monitoimilaitteiden synkronointiasetukset.
Audit Log Management -loki	3001	Tässä lokissa on tietoja, jotka liittyvät tämän toiminnon (Audit Log Management -toiminto) alkamiseen ja päättymiseen, lokien vientiin jne.

Lokeissa voi olla enintään 40 000 tietuetta. Kun tietueiden määrä ylittää 40 000, vanhimmat tietueet poistetaan ensin.

LAITTEIDEN ETÄTUKI

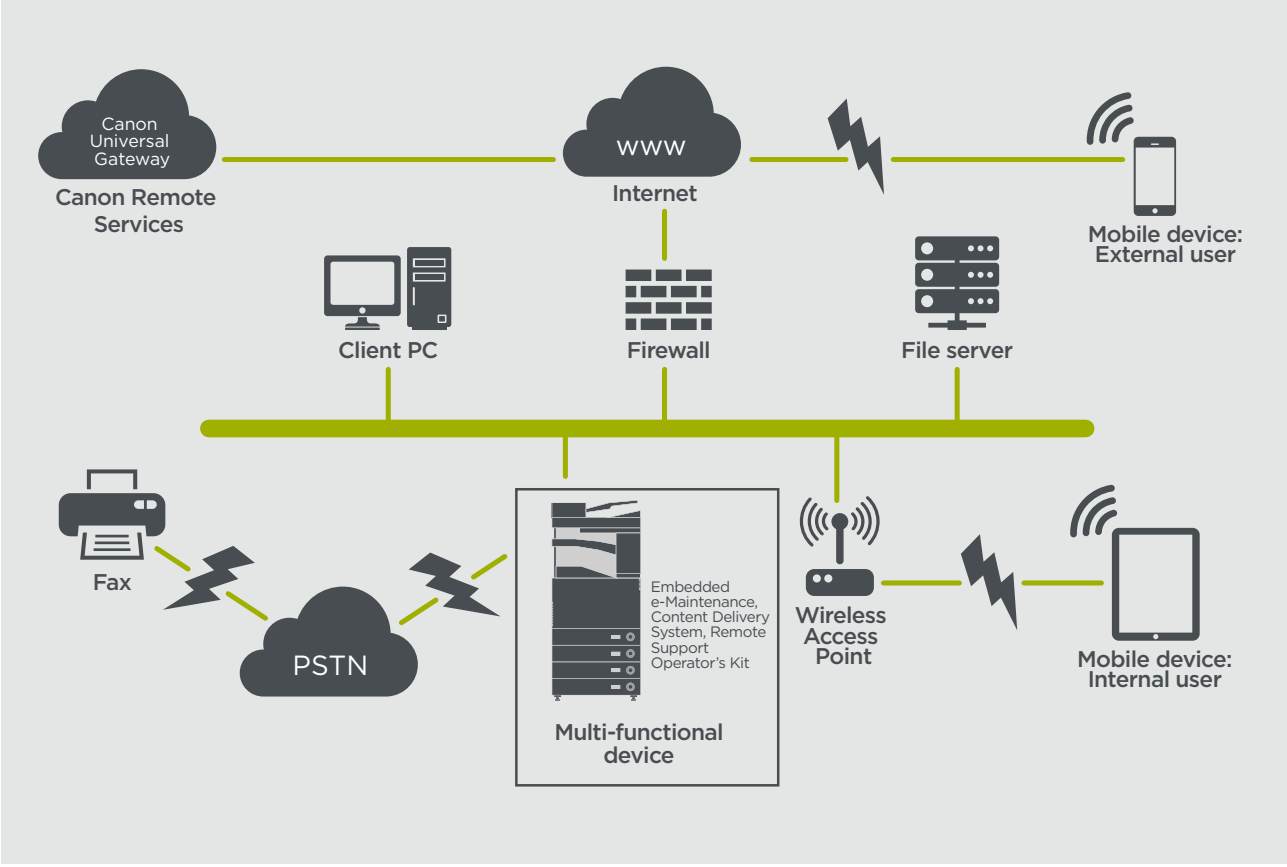
Jotta Canon tai Canon-kumppani voi tarjota tehokasta palvelua, imageRUNNER ADVANCE voi lähettää palveluihin liittyviä tietoja ja vastaanottaa laiteohjelmistopäivityksiä tai ohjelmistosovelluksia. Kuvia tai kuvien metatietoja ei kuitenkaan lähetetä.

Alla on Canonin etäpalvelujen kaksi mahdollista toteutustapaa yrityksen verkossa.

Toteutusskenaario 1: Erilliset yhteydet

Tässä asetuksessa jokainen monitoimilaite sallii suoran yhteyden etäpalveluun Internetin kautta.

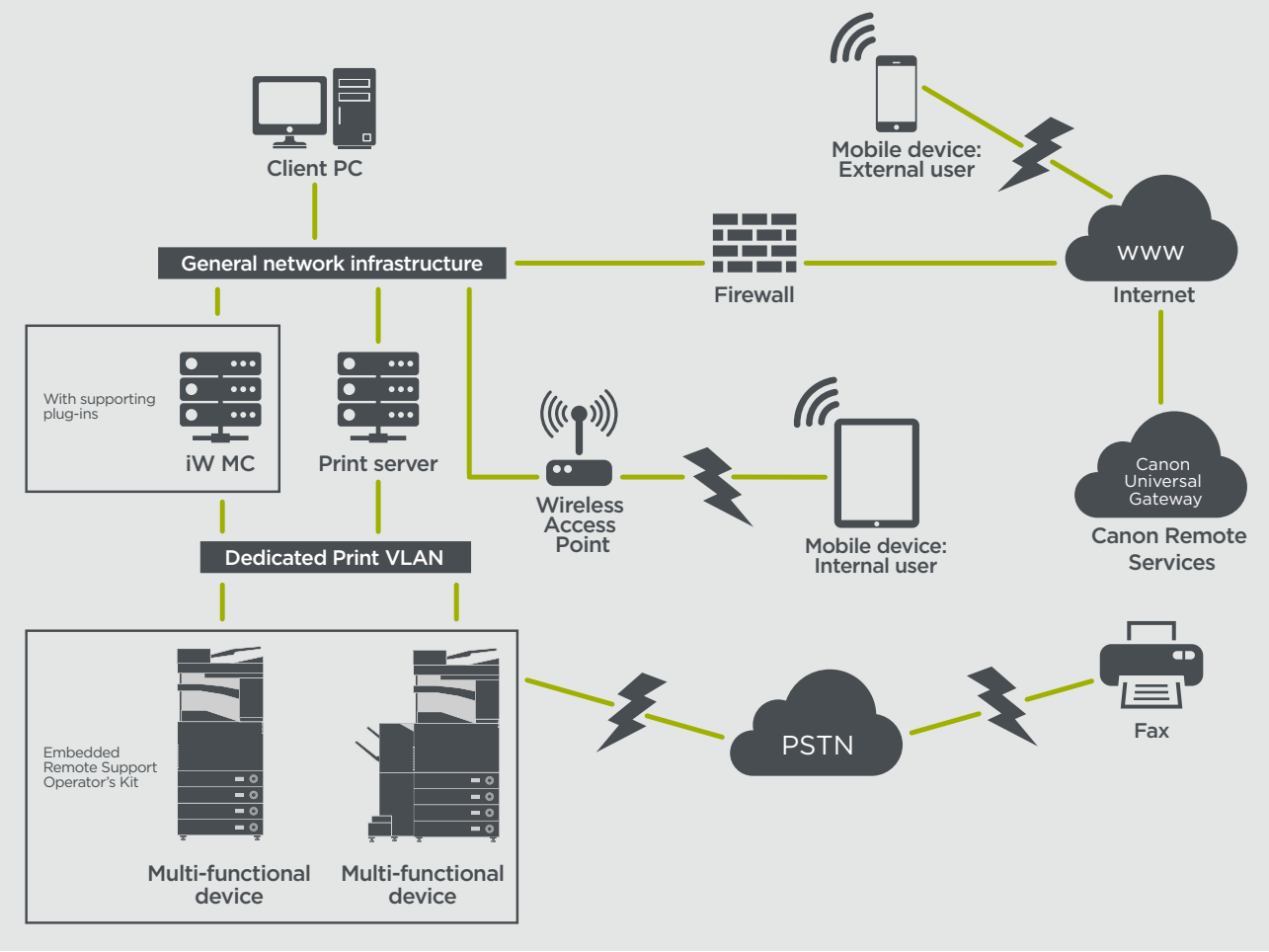
Kuva 9 Erilliset yhteydet



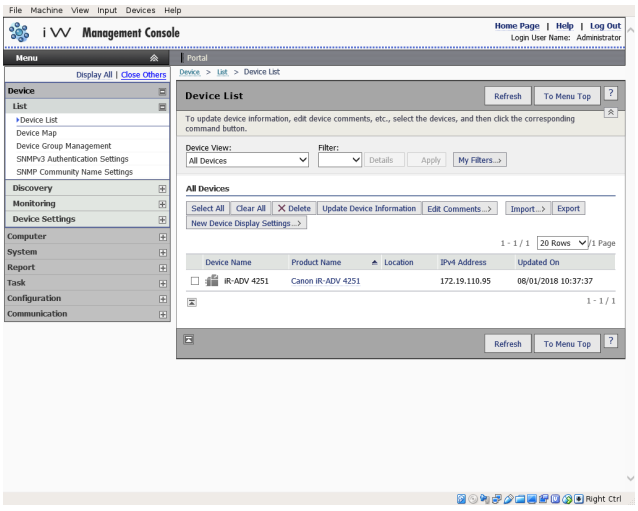
Toteutusskenaario 2: Keskitetty ja hallittu yhteys

Yritysympäristön skenaariossa, jossa on useita monitoimilaitteita, on voitava hallita laitteita tehokkaasti samasta keskitetystä paikasta, ja tämä koskee myös yhteyttä Canonin etäpalveluihin. Jotta kokonaisvaltainen hallintamalli toimii, yksittäiset laitteet muodostavat hallintayhteydet saman iW Management Console (iWMC) -yhteyspisteen kautta. Device Firmware Upgrade (DFU) -laajennuksen ja monitoimilaitteiden välisessä tiedonsiirrossa käytetään UDP-porttia 47545.

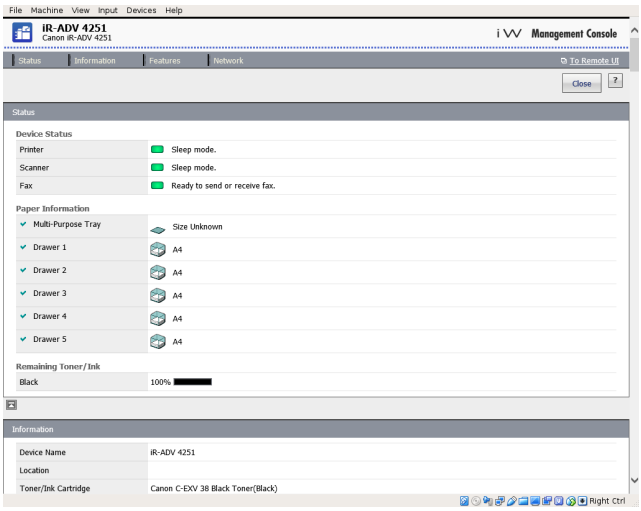
Kuva 10 Keskitetty ja hallittu yhteys



Kuva
11a. Laiteluettelo (tässä tapauksessa yksi laite) imageWARE Management Console -sovelluksessa
11b. Laitteen tiedot ja asetukset



Kuva 11a



Kuva 11b

e-Maintenance

e-Maintenance-järjestelmä tarjoaa automatisoidun keinon kerätä laitteiden käyttölaskuritiedot laskutustietoja, tarvikkeiden hallintaa ja etälaitteiden valvontaa varten tila- ja virhehälytysten avulla.

e-Maintenance-järjestelmässä on internetiin yhteydessä oleva palvelin (UGW) ja sisäinen monitoimilaitteen ohjelmisto (eRDS) ja/tai muu palvelinpohjainen ohjelmisto (RDS-laajennus) laitteen palveluihin liittyvien tietojen keräämiseen. eRDS on valvontaohjelma, joka toimii imageRUNNER ADVANCE -laitteen sisällä. Jos valvonta-asetus on otettu käyttöön laitteen asetuksissa, eRDS hankkii itse laitetiedot ja lähettää ne UGW-palvelimelle. RDS-laajennus on valvontaohjelma, joka asennetaan tavalliseen tietokoneeseen ja jolla voi valvoa 1–3 000 laitetta. Se hankkii tiedot kustakin laitteesta verkon kautta ja lähettää ne UGW-palvelimeen.

Taulukossa 4 on yleiskatsaus siirretyistä tiedoista, protokollista (riippuvat suunnittelun ja käyttöönoton aikana tehdyistä valinnoista) ja käytetyistä porteista. Kopioiden, tulosteiden, skannausten tai faksien kuvatietoja ei siirretä missään vaiheessa.

Taulukko 4 e-Maintenance-tietojen yleiskatsaus

Kuvaus	Käsitellyt tiedot	Protokolla/portti	Portti
Tiedonsiirto e-Maintenancen (eRDS tai RDS-laajennus) ja UGW:n välillä	UGW:n verkkopalvelun osoite Välityspalvelimen osoite / porttinumero Välityspalvelintili / salasana UGW:n postin kohdeosoite SMTP-palvelimen osoite POP-palvelimen osoite Laitteen tila-, laskuri- ja mallitiedot Sarjanumero Jäljellä olevan musteen määrän tiedot Laiteohjelmiston tiedot Korjauspyynnön tiedot Kirjaustiedot Huoltokutsu Palvelun hälytys Tukos Ympäristö Tilaloki	HTTP/HTTPS/SMTP/POP3	TCP/80 TCP/443 TCP/25 TCP/110
Tiedonsiirto e-Maintenancen ja laitteen välillä (vain RDS-laajennus, koska eRDS on sisäinen ohjelmisto)		SNMP Canonin oma SLP/SLP/HTTPS	UDP/161 TCP/47546 UDP/47545, TCP9007 UDP/427 UDP/11427 TCP/443

Sisällönjakelujärjestelmä (Content Delivery System)

Sisällönjakelujärjestelmä (CDS) muodostaa yhteyden monitoimilaitteen ja Canon Universal Gateway (UGW) -palvelimen välille. Se tarjoaa laitteen laiteohjelmisto- ja sovelluspäivitykset.

Taulukko 5 Sisällönjakelujärjestelmän (Content Delivery System) tietojen yleiskatsaus

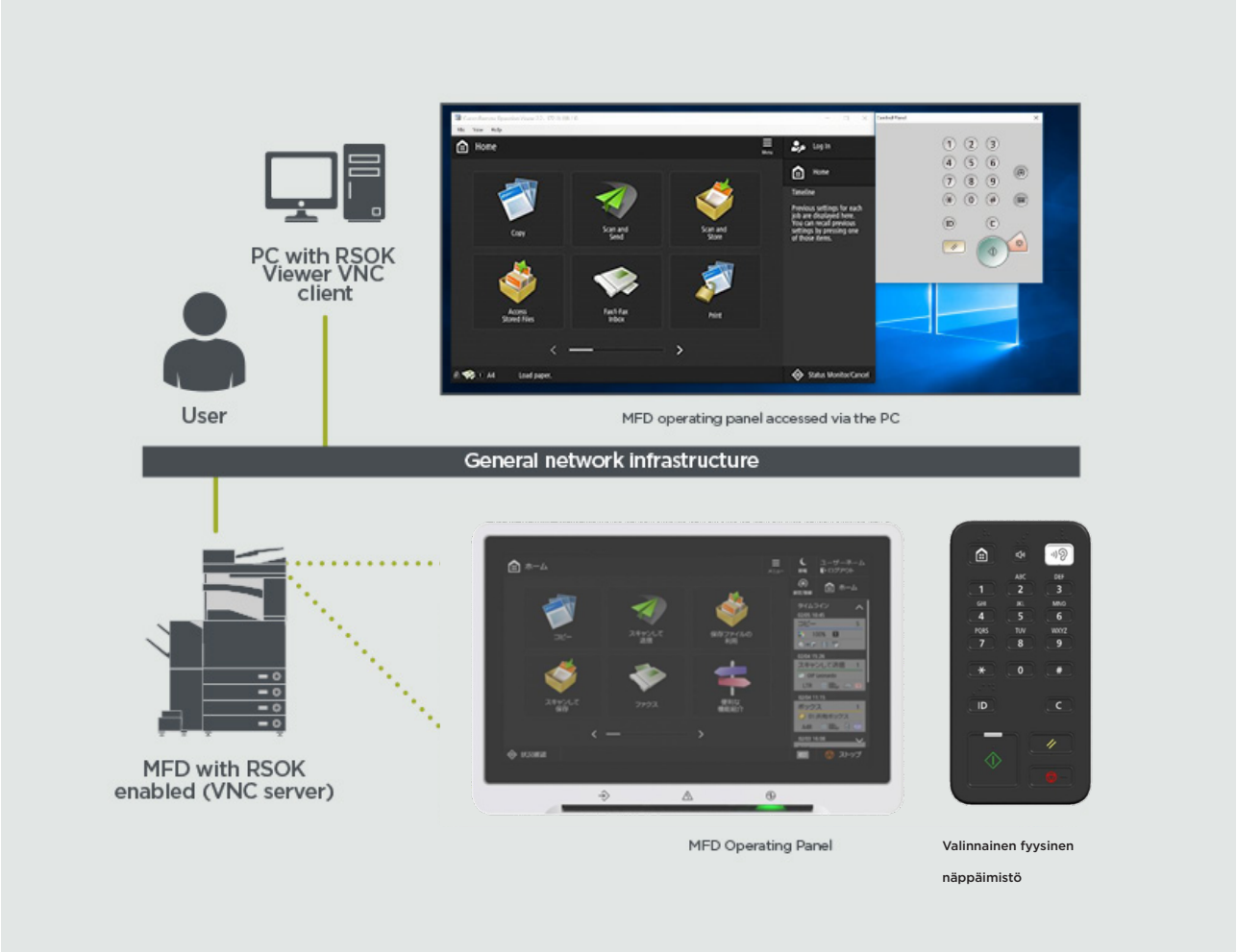
Kuvaus	Lähetetyt tiedot	Protokolla/portti	Portti
Tiedonsiirto monitoimilaitteen ja UGW:n välillä	Laitteen sarjanumero Laiteohjelmistoversio Kieli Maa Laitteen käyttöoikeussopimuksen tiedot	HTTP/HTTPS	TCP/80 TCP/443
Tiedonsiirto UGW:n ja monitoimilaitteen välillä	Yhteystestin testitiedosto (satunnaista binaaridataa) Laiteohjelmiston tai MEAP-sovelluksen binaaridata	HTTP/HTTPS	TCP/80 TCP/443

CDS:n URL-osoite on esimääritettynä laitteen määrityksissä.
Jos halutaan tarjota keskitetty laitteen laiteohjelmistojen ja sovellusten hallinta infrastruktuurin sisältä, tarvitaan iWMC, Laiteohjelmiston päivitys (Device Firmware Upgrade, DFU) -laajennus ja Laitesovellusten hallinta (Device Application Management) -laajennus paikallisesti asennettuina.

Etähallintasovellus (Remote Support Operator's Kit)

Etähallintasovelluksella (RSOK) voi etäkäyttää laitteen ohjauspaneelia. Tässä palvelin-asiakas-järjestelmässä on monitoimilaitteessa toimiva VNC-palvelin ja Microsoft Windowsissa käytettävä etäkäytön katseluohjelman Remote Operation Viewer VNC -asiakassovellus.

Kuva 12 Etähallintasovelluksen (RSOK) asennus



Taulukko 6 Etähallintasovellustietojen yleiskatsaus

Kuvaus	Lähetetyt tiedot	Protokolla/portti	Portti
VNC:n salasanatodennus	Käyttäjän salasana	DES-salaus	5900
Operation Viewer	Laitteen ohjauspaneeli - näytön tiedot - laiteavaimen käyttö	Version 3.3 RFB-protokolla	5900

LIITE

Canon imageRUNNER ADVANCE -laitteen tietoturvaominaisuudet

imageRUNNER ADVANCE -alustalla määritykset voi tehdä verkon kautta käyttöliittymällä, jota kutsutaan etähallintaliittymäksi (Remote User Interface, RUI). Etähallintaliittymässä voi käyttää monia laitteen määritysasetuksia, ja sen voi poistaa käytöstä, jos sitä ei sallita, ja sen voi salasanasuojata luvattoman käytön estämiseksi.

Vaikka suurin osa laitteen asetuksista on käytettävissä etähallintaliittymän kautta, laitteen ohjauspaneelia on käytettävä niiden asetusten määrittämiseen, joita ei voi määrittää etähallintaliittymän kautta. Suosittelemme poistamaan tarpeettomat palvelut käytöstä ja tehostamaan tarpeellisten palvelujen valvontaa. Jotta käyttö on joustavaa ja tukea on saatavilla, Remote Service Operator's Kit (RSOK) -etähallintasovelluksella voi etäkäyttää laitteen ohjauspaneelia. Tämä perustuu VNC-tekniikkaan, jossa on palvelin (monitoimilaite) ja asiakas (verkossa oleva tietokone). Saatavilla on Canonin tietokonesovellus, jolla voi tarvittaessa käyttää ohjauspaneelin painikkeita simuloidusti.

Tässä osassa on yleiskatsaus imageRUNNER ADVANCE -laitteen keskeisistä tietoturvaominaisuuksista ja niiden määritysasetuksista.

Interaktiiviset käyttöoppaat ovat saatavilla verkossa osoitteessa https://oip.manual.canon/, ja niissä on tietoturvaominaisuuksien lisäksi tietoja myös muista ominaisuuksista. Valitse ensin haluamasi tuotetyyppi (esim. imageRUNNER ADVANCE DX), napsauta hakukuvaketta ja kirjoita hakuehdot. Alla on muutamia yleisiä aiheita, joihin kannattaa tutustua.

Laitteen hallinta

Tietovuotojen ja valtuuttamattoman käytön estäminen vaatii jatkuvia ja tehokkaita suojaustoimia. Kun määritetään järjestelmänvalvoja, joka vastaa laitteen asetuksista, käyttäjien hallinnan ja suojausasetusten käyttö voidaan rajata vain valtuutetuille käyttäjille.

Avaa oheinen linkki verkkoselaimessa ja kirjoita hakuruutuun **järjestelmänvalvojan asetukset**. Saat tietoja seuraavista aiheista:

- Laitteen perushallinta
- Laiminlyöntien, käyttäjän virheiden ja väärinkäytön riskien rajoittaminen
- Laitteen hallinta
- Järjestelmän kokoonpanon ja asetusten hallinta

https://oip.manual.canon/USRMA-4879-zz-CS-3700-fiFI/

IEEE P2600 -standardi

Muutamat imageRUNNER ADVANCE -mallit ovat yhteensopivia IEEE P2600 -standardin kanssa, joka on maailmanlaajuisesti käytetty monitoimilaitteiden ja -tulostinten tietoturvastandardi.

Napsauttamalla oheista linkkiä näet IEEE 2600 -standardissa määritetyt tietoturvavaatimukset ja sen, miten laitteen toiminnot täyttävät nämä vaatimukset.
http://ug.oipsrv.net/USRMA-0945-zz-CS-enGB/contents/CT0305_admin_0095.html#345_h1_01

IEEE 802.1X -todennus

Kun halutaan muodostaa yhteys 802.1X-verkkoon, laite on todennettava sen varmistamiseksi, että yhteys on luvallinen.

Avaa oheinen linkki verkkoselaimessa ja kirjoita hakuruutuun **802.1X**.
https://oip.manual.canon/USRMA-4879-zz-CS-3700-fiFI/

Turvallisuuskäytännön käyttäminen laitteessa

Uusimmissa imageRUNNER ADVANCE-malleissa useita laitteen suojausasetuksia voi hallita kootusti turvallisuuskäytäntönä etäkäyttöliittymän kautta. Tässä voidaan käyttää eri salasanaa, jotta vain tietoturvan järjestelmänvalvoja voi muokata näitä asetuksia.

Avaa oheinen linkki verkkoselaimessa ja kirjoita hakuruutuun **turvakäytännön luominen laitteelle**. Saat tietoja seuraavista aiheista:

- Salasanan käyttäminen turvallisuuskäytännön asetusten suojaamiseen
- Turvallisuuskäytännön asetusten määrittäminen
- Turvallisuuskäytännön asetukset

https://oip.manual.canon/USRMA-4879-zz-CS-3700-fiFI/

Käyttäjien hallinta

Asiakkaat, jotka tarvitsevat enemmän suojausta ja tehoa, voivat käyttää sisäistä toimintoa tai tulostuksenhallintaratkaisua, kuten uniFLOW-ratkaisua.

Saat lisätietoja Canonin tulostuksenhallintaratkaisuista ottamalla yhteyttä paikallisiin edustajiimme tai tutustumalla uniFLOW-tuote-esitteeseen.

Verkon suojausasetusten määrittäminen

Valtuutetuille käyttäjille voi aiheutua odottamattomia menetyksiä epärehellisten kolmansien osapuolten hyökkäyksistä, kuten verkossa siirrettävien tietojen vakoilusta, väärentämisestä ja peukaloinnista. Jotta tärkeitä ja arvokkaita tietoja voidaan suojata näiltä hyökkäyksiltä, laitteessa on useita turvallisuutta ja tietosuojaa edistäviä ominaisuuksia.

Avaa oheinen linkki verkkoselaimessa ja kirjoita hakuruutuun **verkon suojausasetusten määrittäminen**. Saat tietoja seuraavista aiheista:

Linkin kautta saat seuraavia tietoja:

- Luvattoman käytön estäminen
- Langattomaan lähiverkkoon yhdistäminen
- Verkkoympäristön määrittäminen

https://oip.manual.canon/USRMA-4879-zz-CS-3700-fiFI/

Kiintolevyn tietojen hallinta

Laitteen kiintolevylle tallennetaan laitteen käyttöjärjestelmä, määritysasetukset ja töiden tiedot. Useimmissa laitemalleissa käytetään koko levyn salausta (FIPS 140-2 -yhteensopiva), joka koskee vain tiettyä laitetta ja estää tietojen valtuuttamattoman lukemisen. Canon MFP Security Chip on salausmoduuli, jolla on Yhdysvalloissa ja Kanadassa määritetty CMVP (Cryptographic Module Validation Program) -sertifiointi sekä JCMVP (Japan Cryptographic Module Validation Program) -sertifiointi.

Avaa oheinen linkki verkkoselaimessa ja kirjoita hakuruutuun **kiintolevyn tietojen hallitseminen**.

https://oip.manual.canon/USRMA-4879-zz-CS-3700-fiFI/

TURVALLISUUSKÄYTÄNNÖN ASETUSTEN YLEISKATSAUS

imageRUNNER ADVANCE -mallien kolmannen sukupolven malleissa on turvallisuuskäytännön asetukset ja tietoturvan järjestelmänvalvoja. Laite vaatii järjestelmänvalvojan kirjautumisen sekä erillisen tietoturvan järjestelmänvalvojan kirjautumisen omalla salasanalla, jos tämä on määritetty.

Oheisessa taulukossa on kuvattu käytettävissä olevat asetukset.

1. Interface	Huomautukset
Wireless Connection Policy	
Prohibit Use of Direct Connection	<Use Wi-Fi Direct> -asetuksena on <Off>. Laitetta ei voi käyttää mobiililaitteiden avulla.
Prohibit Use of Wireless LAN	<Select Wired/Wireless LAN> -asetuksena on <Wired LAN>. Laitteeseen ei voi muodostaa langatonta yhteyttä langattoman lähiverkon reitittimen tai tukiaseman kautta.
USB -käytäntö	
Estä käyttö USB-laitteena	<Käytä USB-laitteena/Use as USB Device> -asetus on tilassa <Ei käytössä/Off> Et voi käyttää tulostus- tai skannaustoimintoja USB-liitäntään kytketyistä tietokoneista, kun USB-laitteen käyttö on kielletty.
Estä käyttö USB-tallennuslaitteena	<Käytä USB-tallennuslaitteena> -asetus on <Ei käytössä/Off>. USB-muistilaitteita ei voi käyttää Seuraavien palvelujen toiminnot kuitenkin toimivat, vaikka "Estä käyttö USB -tallennuslaitteena" on valittu: • Laiteohjelmistopäivitys USB-tikun kautta (lataustilassa) • Sublog-tietojen kopiointi laitteesta USB-laitteeseen (LOG2USB) • Raportin kopiointi laitteesta USB-laitteeseen (RPT2USB)
Verkon tiedonsiirron toteutuskäytäntö (Network Communication Operational Policy) Huomautus: nämä asetukset eivät koske tiedonsiirtoa IEEE 802.1X -verkkojen kanssa, vaikka [Todenna aina palvelinvarmenne TLS:ää käytettäessä/Always Verify Server Certificate When Using TLS] -valintaruutu on valittu.	
Tarkista aina SMS-/WebDAVpalvelintoimintojen allekirjoitukset	<SMB -palvelinasetukset> -kohdan <Vaadi yhteydeltä SMB-allekirjoitus>- ja <Käytä SMB -todennusta> -asetuksena on <Käytössä>, ja <WebDAV -palvelinasetukset> -kohdan <Käytä TLS:ää> -asetuksena on <Käytössä> Kun laitetta käytetään SMB-palvelimena tai WebDAV-palvelimena, digitaalisten varmenteiden allekirjoitukset vahvistetaan tiedonsiirron aikana.
Todenna aina palvelinvarmenne TLS:ää käytettäessä	<Vahvista TLS-varmenne WebDAV TX:lle>-, <Vahvista TLS-varmenne SMTP TX:lle>-, <Vahvista TLS -varmenne POP RX:lle>-, <Vahvista TLS-varmenne verkkokäytölle>- ja <Vahvista TLS-varmenne käyttämällä MEAP-sovellusta> -asetuksena on <Käytössä>, ja tarkistusmerkki on lisätty kohtaan <CN> Tämän lisäksi <Todenna palvelinvarmenne> ja <Todenna CN> -asetuksiksi kohdissa <SIP-asetukset> ><TLS-asetukset> on määritetty <Käytössä>. Digitaaliset varmenteet ja niiden yleiset nimet vahvistetaan TLS-tiedonsiirron aikana.
Estä selväkielisen tekstin todennus palvelintoiminnoille	• <FTP-tulostusasetukset> -kohdan <Käytä FTP-tulostusta> -asetukseksi on määritetty <Ei käytössä> • <Salli TLS (SMTP RX)> kohdassa <Sähköposti-/I-Fax-asetukset> <Tiedonsiirtoasetukset> -asetuksiksi on määritetty <Aina TLS>, <Erillinen portin todennusmenetelmä> -asetukseksi kohdassa <Verkko> on asetettu <Tila 2>, • <WebDAV-palvelinasetukset> -kohdan <Käytä TLS:ää> -asetukseksi on määritetty <Käytössä> Kun laitetta käytetään palvelimena, toiminnot, jotka käyttävät selväkielistä todennusta, eivät ole käytettävissä. TLS:ää käytetään, jos selväkielinen todennus on kielletty. Tämän lisäksi ei ole mahdollista käyttää sellaisia sovelluksia tai palvelimen toimintoja, kuten FTP:tä, jotka tukevat pelkkää selväkielistä todennusta. Laitetta ei välttämättä voi käyttää laitteen hallintaohjelmiston tai ohjaimen avulla.
Estä SNMPv1:n käyttö	<SNMP-asetukset> -kohdassa <Käytä SNMPv1:tä> -asetukseksi on määritetty <Ei käytössä>. Laitteen tietoja ei välttämättä voi noutaa eikä määrittää tulostinohjaimen tai hallintaohjelman avulla, jos SNMPv1 on kielletty.
Portin käyttöä koskeva käytäntö	
Rajoita LPD-portin käyttöä	Porttinumero 515 <LPD-tulostusasetukset> -kohdan asetukseksi on määritetty <Ei käytössä>. LPD-tulostusta ei voi suorittaa.
Rajoita RAW-portin käyttöä	Porttinumero 9100 <RAW-tulostusasetukset> -kohdan asetukseksi on määritetty <Ei käytössä>. RAW-tulostusta ei voi suorittaa.
Rajoita FTP-portin käyttöä	Porttinumero 21 <FTP-tulostusasetukset> -kohdan <Käytä FTP-tulostusta> -asetukseksi on määritetty <Ei käytössä>. FTP-tulostusta ei voi suorittaa.
Rajoita WSD-portin käyttöä	Porttinumerot 3702, 60000 <WSD-asetukset> -kohdassa <Käytä WSD:tä>, <Käytä WSD-selausta> ja <Käytä WSD-skannausta> -asetuksiksi on määritetty <Ei käytössä>. WSD-toimintoja ei voi käyttää.
Rajoita BMLinkS-portin käyttöä	Porttinumero 1900 Ei käytössä Euroopassa.

Rajoita IPP-portin käyttöä	Porttinumero 631 Mopriaa, AirPrintiä tai IPP:tä ei voi käyttää, jos IPP-portin käyttöä on rajoitettu.
Rajoita SMB-portin käyttöä	Porttinumerot 137, 138, 139, 445 <SMB-palvelinasetukset> -kohdassa <Käytä SMB-palvelinta> -asetukseksi on määritetty <Ei käytössä> Laitetta ei voi käyttää SMB-palvelimena.
Rajoita SMTP-portin käyttöä	Porttinumero 25 <Sähköposti-/I-Fax-asetukset> -kohdassa > <Tiedonsiirtoasetukset>, <SMTP RX> -asetukseksi on määritetty <Ei käytössä> SMTP-vastaanotto ei ole mahdollinen.
Rajoita erillisen portin käyttöä	Porttinumerot: 9002, 9006, 9007, 9011-9015, 9017-9019, 9022, 9023, 9025, 20317, 47545–47547 Etätulostuksen, etäfaksin, etäskannauksen tai etätulostuksen toimintoja tai sovelluksia jne. ei voi käyttää, jos niille varatun portin käyttöä on rajoitettu.
Rajoita etäkäyttäjän ohjelmistoportin käyttöä	Porttinumero 5900 <Etäkäyttöasetukset> -kohdan asetukseksi on määritetty <Ei käytössä> Etäkäytön toimintoja ei voi käyttää.
Rajoita SIP (IP-faksi) -portin käyttöä	Porttinumerot 5004, 5005, 5060, 5061, 49152 <Käytä Intranetiä> -asetukseksi kohdassa <Intranet-asetukset>, <Käytä NGN:ää> -asetukseksi kohdassa <NGN-asetukset> ja <Käytä VoIP-yhdyskäytävää> -asetukseksi kohdassa <VoIP-yhdyskäytäväasetukset> on määritetty <Ei käytössä>. IP-faksia ei voi käyttää.
Rajoita mDNS-portin käyttöä	Porttinumero 5353 <mDNS-asetukset> -kohdassa <Käytä IPv4 mDNS:ää> ja <Käytä IPv6 mDNS:ää> -asetuksiksi on määritetty <Ei käytössä> <Käytä Mopriaa> -asetuksena on <Ei käytössä>. Verkossa ei voi tehdä hakuja eikä automaattisia asetuksia voi määrittää mDNS-palvelulla. Mopria™- tai AirPrint-toiminnolla ei voi tulostaa.
Rajoita SLP-portin käyttöä	Porttinumero 427 <Monilähetyksen havaitsemisasetukset> -kohdassa <Vastaus> -asetukseksi on määritetty <Ei käytössä>. Verkossa ei voi tehdä hakuja eikä automaattisia asetuksia voi määrittää käyttämällä SLP:tä.
Rajoita SNMP-portin käyttöä	Porttinumero 161 Laitteen tietoja ei välttämättä voi noutaa eikä määrittää tulostinohjaimen tai hallintaohjelman avulla, jos SNMP-portin käyttöä on rajoitettu. <SNMP-asetukset> -kohdassa <Käytä SNMPv1:tä> ja <Käytä SNMPv3:a> -asetuksiksi on määritetty <Ei käytössä>

2. Todennus	Huomautukset
Todennuksen käyttöä koskeva käytäntö	
Estä vieraskäyttäjät	• <Lisätila-asetukset> > <Todennuksien hallinta> -asetukseksi on määritetty <Käytössä> • <Kirjautumisnäytön näyttöasetukset> -asetukseksi on määritetty <Näytä laitteen käynnistyessä> • <Rajoita työn käyttöä etälaitteelta ilman käyttäjän todennusta> -asetukseksi on määritetty <Käytössä> Rekisteröitymättömät käyttäjät eivät voi kirjautua laitteeseen. Myös tietokoneesta lähetetyt tulostustyöt peruutetaan.
Pakota automaattisen uloskirjautumisen asetus	Tämä asetus on tarkoitettu ohjauspaneelista uloskirjaamiseen. Tämä ei koske muita uloskirjauksen menetelmiä (määritettävä aika 10 sekuntia – 9 minuuttia). <Automaattinen nollausaika> on käytössä. Käyttäjä kirjataan automaattisesti ulos, mikäli mitään toimintoa ei suoriteta tiettyyn ajanjaksoon. Valitse etäkäyttöliittymän asetusnäytössä [Aika uloskirjautumiseen].
Salasanan käyttöä koskeva käytäntö	
Estä ulkoisten palvelimien salasanojen tallennus välimuistiin	Tämä asetus ei koske salasanoja, jotka käyttäjä tallentaa erikseen, kuten osoitekirjojen salasanoja jne. <Estä ulkoisten palvelimien salasanojen tallennus välimuistiin> -asetukseksi on määritetty <Käytössä>. Käyttäjiä vaaditaan aina antamaan salasana, kun he käyttävät ulkoista palvelinta.
Näytä varoitus, kun oletussalasana on käytössä	<Näytä varoitus, kun oletussalasana on käytössä> -asetukseksi on määritetty <Käytössä>. Varoitusviesti näkyy, kun laitteen oletussalasanaa käytetään.
Estä oletussalasanan käyttö etäyhteyden välityksellä tapahtuvalle käytölle	<Salli oletussalasanan käyttö etäkäyttöä varten> -asetukseksi on määritetty <Ei käytössä>. Oletussalasanaa ei voi käyttää, kun laitetta käytetään tietokoneesta.
Salasana-asetusten käytäntö (Käytäntö ei koske osaston tunnusten hallintaa tai PIN-koodia)	
Aseta salasanan vähimmäismerkkimäärä	Merkkien vähimmäismääräksi voi määrittää 1–32.
Määritä salasanan voimassaoloaika	Voimassaoloajaksi voi määrittää 1–180 päivää.
Estä kolmen tai useamman identtisen merkin käyttö peräkkäin	
Pakota vähintään 1 ison kirjaimen käyttö	
Pakota vähintään 1 pienen kirjaimen käyttö	
Pakota vähintään 1 numeron käyttö	
Pakota vähintään 1 symbolin käyttö	
Lukituskäytäntö	
Ota lukitus käyttöön	Ei koske osastotunnusta / postilaatikon PIN-koodia, PIN-koodia eikä turvatulostuksen todennusta jne. Lukituksen raja-arvo: arvoksi voi määrittää 1–10 kertaa. Lukitusjakso: arvoksi voi määrittää 1–60 minuuttia.

3. Avain/varmenne	Huomautukset
Estä heikon salauksen käyttö	Koskee seuraavia: IPSec, TLS, Kerberos, S/MIME, SNMPv3 ja langaton lähiverkko. Tiedonsiirto ei välttämättä toimi sellaisten laitteiden kanssa, jotka tukevat vain heikkoa salausta.
Estä avaimen/varmenteen käyttö heikon salauksen kanssa	Koskee seuraavia: IPSec, TLS ja S/MIME. Jos TLS:ssä käytetään avainta/varmennetta, jossa on heikko salaus, se vaihdetaan esiasennettuun avaimeen/varmenteeseen. Tiedonsiirto ei toimi, jos käytetään avainta/varmennetta, jossa on heikko salaus, muihin toimintoihin kuin TLS:ään.
Käytä TPM:ää salasanan ja avaimen tallentamiseen	Käytettävissä vain laitteille, joihin on asennettu TPM. Varmuuskopioi aina TPM-avaimet, kun TPM on otettu käyttöön. Katso lisätietoja käyttöoppaasta. Tärkeää, kun TPM-asetukset on otettu käyttöön: • Varmista, että muutat järjestelmänvalvojan salasanan oletusarvosta, jotta estät sen, että kolmas osapuoli voi varmuuskopioida TPM-avaimen. Jos kolmas osapuoli saa TPM-avaimen varmuuskopion, et voi palauttaa TPM-avainta. • Turvallisuuden parantamiseksi TPM-avaimen voi varmuuskopioida vain kerran. Jos TPM-asetukset on otettu käyttöön, varmista, että varmuuskopioit TPM-avaimen USB-muistilaitteelle ja säilytät sitä turvallisessa paikassa, jotta se ei katoa eikä sitä voi varastaa. • TPM:n tarjoamat suojaustoiminnot eivät takaa tietojen ja laitteiston täydellistä turvaa.

4. Loki	Huomautukset
Pakota valvontalokin tallennus	• <Tallenna käyttöloki> -asetukseksi on määritetty <Käytössä> • <Näytä työloki> -asetukseksi on määritetty <Käytössä> • <Nouda työloki hallintaohjelmiston avulla> -asetukseksi on <Näytä työloki> -kohdassa määritetty <Salli>. • <Tallenna valvontaloki> -asetukseksi on määritetty <Käytössä> • <Nouda verkon todennusloki> -asetukseksi on määritetty <Käytössä> Tarkastuslokit tallennetaan aina, kun tämä asetus on otettu käyttöön.
Pakota SNTP-asetukset	Anna SNTP-palvelimen osoite. <SNTP-asetukset> -kohdassa <Käytä SNTP:tä> -asetukseksi on määritetty <Käytössä>. Ajan synkronointi SNTP:n kautta vaaditaan. Anna arvo etäkäyttöliittymän asetusnäytön [Palvelinnimi] -kohtaan.
Syslog -lokitietojen raportointi	Ota käyttöön Syslogin kohdetiedot, kun käytät Syslog-palvelinta tai SIEM-järjestelmää. • <Käyttäjänimi ja salasana> • <SMB palvelinnimi> • <Kohdeosoite> • <Lähetysaika>

5. Työ	Huomautukset
Tulostuskäytäntö	
Estä vastaanotettujen töiden välitön tulostaminen	Vastaanotetut työt tallennetaan faksin/I-faksin muistiin, jos vastaanotettujen töiden välitön tulostus on kielletty. • <Käsittele tiedostoja, joissa edelleenlähetysvirheitä> -asetukseksi on määritetty <Ei käytössä> • <Käytä faksin muistin lukitusta> -asetukseksi on määritetty <Käytössä> • <Käytä I-Faxin muistin lukitusta> -asetukseksi on määritetty <Käytössä> • <Muistin lukituksen päättymisaika> -asetukseksi on määritetty <Ei käytössä> • <Näytä tuloste tallennettaessa tulostinohjaimelta> -asetukseksi kohdassa <Aseta/rekisteröi luottamuksellisia faksilaatikoita> on asetettu <Ei käytössä> • <Asetukset kaikille postilaatikoille> > <Tulosta tallennettaessa tulostinohjaimelta> -asetukseksi on määritetty <Ei käytössä> • <Laatikon tietoturva-asetukset> > <Näytä tuloste tallennettaessa tulostinohjaimelta> -asetukseksi on määritetty <Ei käytössä> • <Estä työ tuntemattomalta käyttäjältä> -asetukseksi on määritetty <Käytössä> ja <Pakotettu pito> -asetukseksi on määritetty <Käytössä>. Tulostus ei tapahdu välittömästi, vaikka tulostustoimintoja suoritettaisiin.
Lähetys-/vastaanottokäytäntö	
Salli lähettäminen vain rekisteröityihin osoitteisiin	<Rajoita uutta kohdetta> -kohdassa <Faksi>-, <Sähköposti>-, <I-Fax>- ja <Tiedosto>-asetuksiksi on määritetty <Käytössä>. Lähettäminen on mahdollista vain kohteisiin, jotka ovat osoitekirjassa.
Pakota faksinumeron vahvistus	Käyttäjien on annettava faksinumero uudelleen vahvistusta varten, kun he lähettävät faksin.
Estä automaattinen edelleenlähetys	<Käytä edelleenlähetysasetuksia> -asetukseksi on määritetty <Ei käytössä>. Fakseja ei voi ohjata automaattisesti uudelleen.

6. Tallennustila	Huomautukset
Pakota tietojen lopullinen poisto	<Kiintolevyn tietojen pysyvä poisto> -asetukseksi on määritetty <Käytössä>

Katso imageRUNNER ADVANCE -laitteen tekniset tiedot tuotteen verkkosivustolta osoitteesta
https://www.canon-europe.com/business-printers-and-faxes/imagerunner-advance-dx/.

Canon Oy
Huopalahdentie 24
00350 HELSINKI

Puhelin: 010 54420

canon.fi

Canon Inc.
Canon.com

Canon Europe / Canon Oy
canon-europe.com

Finnish edition v1.0