



Canon

INFORMATIEBEVEILIGING MET CANON eMAINTENANCE

Canon's eMaintenance zorgt voor het beheer en de verwerking van al uw Canon MFP- en SFP-apparaten in het netwerk en houdt zich daarbij aan strikte beveiligingsprotocollen.



DEEL 1: VEELGESTELDE VRAGEN

Dit document is bedoeld om antwoord te geven op de belangrijkste beveiligingsvragen die u mogelijk hebt over eMaintenance. Neem voor meer informatie over de beveiliging die is opgenomen in eMaintenance contact op met uw plaatselijke Canon-vertegenwoordiger.



Wie is de eigenaar van mijn gegevens?

In alle gevallen zijn uw gegevens eigendom van u. Canon is slechts een overeengekomen gegevensverwerker van de eMaintenance-gegevens van klanten.



Wie heeft toegang tot mijn gegevens?

Canon biedt een gelaagde benadering voor het reguleren van de toegang tot gegevens, waaronder:

- **Controle op fysieke toegang:** Alleen bevoegde personen hebben fysieke toegang tot kantoren, gebouwen of ruimten waar persoonsgegevens zijn opgeslagen.
- **Controle op systeemtoegang:** Systemen waarop persoonsgegevens worden verwerkt, zijn alleen toegankelijk met autorisatie op basis van gebruikersrollen en bijbehorende machtigingen.
- **Controle op gegevenstoegang:** Personen die het recht hebben om gegevensverwerkingssystemen te gebruiken, krijgen alleen toegang tot de persoonsgegevens waartoe zij recht hebben.
- **Controle op gegevensoverdracht:** Behalve voor zover nodig voor de levering van services in overeenstemming met de relevante overeenkomst, mogen persoonsgegevens niet worden gelezen, gekopieerd, gewijzigd of verwijderd zonder toestemming tijdens de overdracht:
- **Controle op gegevensinvoer:** Canon implementeert maatregelen die het mogelijk maken om met terugwerkende kracht te onderzoeken en vast te stellen of en door wie persoonsgegevens zijn ingevoerd, gewijzigd of verwijderd uit de gegevensverwerkingssystemen van Canon.
- **Controle op functies:** Alle Canon-werknemers en contractuele subverwerkers of andere serviceproviders zijn contractueel gebonden om de vertrouwelijkheid van alle gevoelige informatie te respecteren.
- **Controle op scheiding van gegevens:** Persoonsgegevens worden alleen opgeslagen en zijn alleen toegankelijk vanaf de individuele eMaintenance-tenant van elke klant.

De toegang tot gegevens wordt geregeld met behulp van de volgende maatregelen:

- Als onderdeel van het beveiligingsbeleid van Canon is voor persoonsgegevens ten minste hetzelfde beschermingsniveau vereist als voor "vertrouwelijke" informatie.
- Toegang tot persoonsgegevens wordt verleend op basis van need-to-know. Personeelsleden hebben toegang tot de informatie die zij nodig hebben om hun taken uit te voeren.
- Beveiligingsmaatregelen ter bescherming van toepassingen die persoonsgegevens verwerken, worden regelmatig nagelopen. Daarom voert Canon interne en externe beveiligingscontroles en penetratietests uit op haar IT-systemen.
- Persoonsgegevens mogen niet zonder toestemming worden gelezen, gekopieerd, gewijzigd of verwijderd tijdens de verwerking, het gebruik en de opslag.



Zijn mijn gegevens versleuteld?

Gegevens die zijn opgeslagen in de AWS-cloudservice worden versleuteld.

Wanneer gegevens worden overgedragen tussen Canon en haar klanten, wordt dit altijd uitgevoerd via beveiligde versleutelingsprotocollen.

Persoonsgegevens die kunnen worden opgeslagen bij gebruik van de optionele Data Backup Service of Installation Support Service, zoals adresboekgegevens van het apparaat, worden versleuteld met AES-256.



Hoe worden mijn gegevens gescheiden van de gegevens van andere klanten?

Persoonsgegevens worden met de volgende scheidingsmaatregelen verwerkt:

Canon gebruikt de juiste technische controlemechanismen om de gegevens van de klant logisch te scheiden.

Indien van toepassing zorgt een boomstructuur met meerdere lagen ervoor dat de tenant van een bovenliggend item toegang heeft tot de tenant van de onderliggende items, maar de onderliggende items hebben geen toegang tot andere tenants op hetzelfde of een hoger niveau (zoals de bovenliggende items).



Welke gegevens worden verzameld door eMaintenance?

De meeste gegevens die worden verzameld en gebruikt door eMaintenance zijn niet-persoonlijk identificeerbare apparaatgegevens zoals klant, apparaatnaam, serienummer, locatie, IP-adres, status en waarschuwingen.

De volgende informatie wordt niet verzameld door eMaintenance: informatie met betrekking tot het gebruik, zoals gebruikersnaam*, datum/tijd, documentnaam, taakinhoud (beeldgegevens/printgegevens) voor KOPIËREN, PRINTEN, SCANNEN en VERZENDEN.



Controleert Canon de cloudbeveiliging?

Canon voert diverse audits uit als indicatoren van de implementatiestatus van de informatiebeveiliging van de cloudservices die Canon biedt, om ervoor te zorgen dat Canon en haar klanten de services vol vertrouwen kunnen gebruiken.

Om de beveiligingsmaatregelen van eMaintenance te controleren, worden er regelmatig penetratietests uitgevoerd door een derde partij.

*Wanneer u de optionele Data Backup Service of Installation Support Service gebruikt, kunnen persoonsgegevens zoals gebruikersnaam en e-mailadres worden verzameld als deze zijn opgenomen in het adresboek van het apparaat, maar alleen met specifieke toestemming van de klant.





Is de eMaintenance-cloudinfrastructuur veilig?

De eMaintenance-service wordt gehost op het AWS-platform in Frankfurt in Duitsland.



Heeft eMaintenance een certificering voor een belangrijke beveiligingsstandaard?

Het Digital Printing Development Center van Canon Inc. is gecertificeerd volgens de internationale standaard ISO/IEC 27001. Deze certificering heeft betrekking op de ontwikkeling van Canon Inc. van de monitoringservice (inclusief eMaintenance Suite) voor multifunctionele apparaten (MFD's) en printers.

Dankzij de ISO/IEC 27001- en ISO/IEC 27017-certificering kan Canon Inc. bevestigen dat haar beveiligingsprocessen zijn gecertificeerd door derden volgens een internationaal erkende standaard.

Deze standaard laat zien dat Canon Inc. zich inzet voor informatiebeveiliging binnen de organisatie en het online serviceaanbod:

- **Vertrouwelijkheid:** de garantie dat informatie alleen toegankelijk is voor personen die daartoe gemachtigd zijn.
- **Integriteit:** bescherming van de juistheid en volledigheid van informatie en verwerkingsmethoden.
- **Beschikbaarheid:** de garantie dat geautoriseerde gebruikers toegang hebben tot informatie wanneer dat nodig is.



Voor ISO/IEC 27001 is regelmatige beoordeling vereist. Dit betekent dat de functies van de monitoringservice worden ontwikkeld en geleverd door een veilige organisatie, hetgeen wordt bevestigd door certificering door derden volgens overeengekomen internationale normen.

ISO/IEC 27017 is een uitbreiding van ISO/IEC 27001 en definieert aanvullende beveiligingsmaatregelen die specifiek zijn bedoeld voor cloudserviceproviders. Hierin is een informatiebeveiligingskader opgenomen voor organisaties die cloudservices gebruiken.

Canon heeft ervoor gekozen om te voldoen aan deze gedragscode voor informatiebeveiligingscontroles, omdat hun cloudserviceklanten hierdoor beveiligd worden dankzij een consistente en uitgebreide benadering van informatiebeveiliging.

VERKLARENDE WOORDENLIJST

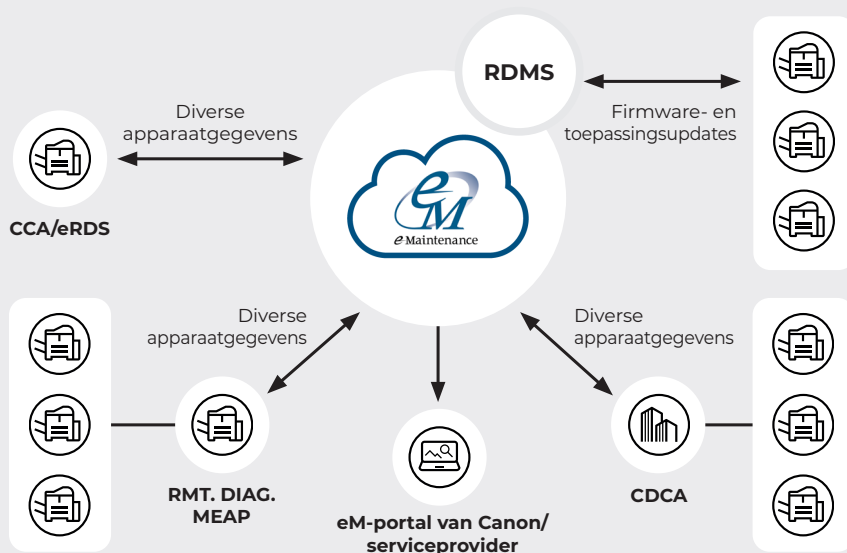
CCA: Cloud Connection Agent

CDCA: Canon Data Collection Agent

RMT. DIAG. MEAP: Remote Diagnostics MEAP

eRDS: embedded Remote Diagnostic System

RDMS: Remote Distribution & Management Service



DEEL 2: INFRASTRUCTUURVEREISTEN eM

eM maakt gebruik van een aantal lokale agents en softwaretoepassingen voor communicatie tussen de Canon-apparaten en de eM-service. Afhankelijk van een aantal factoren, zoals het type apparaat, de lokale infrastructuur en de servicevereisten, kan elke klant een of meer van deze opties laten inschakelen.

De opties zijn als volgt:

CCA (Cloud Connection Agent)

CCA is de recentste ingebouwde agent voor eMaintenance. Deze wordt intern op het apparaat uitgevoerd zonder dat er een afzonderlijke agent voor gegevensverzameling op uw netwerk hoeft te worden geïnstalleerd. Omdat het apparaat een breder scala aan apparaatgegevens kan verzamelen, is CCA-connectiviteit vereist om te profiteren van de nieuwste (en toekomstige) eMaintenance-functionaliteit en -services, waaronder AI-gebaseerde voorspellende diagnose en reparatie. CCA kan worden toegevoegd aan bestaande apparaten met eRDS.

CDCA (Canon Data Collection Agent)

Dit is een op de pc geïnstalleerde agent voor eMaintenance. Deze monitoringsoftware wordt geïnstalleerd op een lokale pc in het netwerk van de klant.

RMT. DIAG. MEAP (Remote Diagnostics MEAP)

Dit is ingebouwde agentsoftware voor eMaintenance die gebruik maakt van het MEAP-platform, waarmee het hostapparaat en andere Canon-apparaten op het netwerk kunnen worden bewaakt. Ideaal voor kleinere netwerken waarvoor geen CDCA-server nodig is.

eRDS (embedded Remote Diagnostic Service)

eRDS is een oudere ingebouwde agent voor eMaintenance. Deze monitoringsoftware wordt intern op het apparaat zelf uitgevoerd. eRDS verzendt apparaatbeheerinformatie naar de eMaintenance-service en kan worden ingesteld om updates van firmware en MEAP-toepassingslicenties te ontvangen.

RDMS (Remote Distribution & Management Service)

Hiermee kunnen geautoriseerde Canon-serviceproviders producten en licenties voor MEAP-toepassingen en iR-opties beheren en firmware- en MEAP-toepassingslicenties bijwerken.

Data Backup Service

Deze optionele service maakt regelmatig een geplande back-up van de instellingen die op het interne opslagapparaat staan en slaat deze in gecodeerde vorm op in de cloud. Als de HDD/SSD/controller defect raakt en moet worden vervangen, kan de Data Backup Service de gegevens naar het apparaat herstellen, waardoor de reparatietijd aanzienlijk wordt verkort.

Vereiste netwerktoegang

Om eMaintenance te laten functioneren, wordt klanten gevraagd om de Canon-apparaten toegang te verlenen via de juiste URL's die via hun netwerk beschikbaar zijn. Vraag uw Canon-vertegenwoordiger naar de lijst met specifieke URL's die vereist zijn voor uw omgeving.

AFZONDERLIJKE URL'S VOOR eMAINTENANCE-VERBINDING

Canon raadt het gebruik van
jokertekens aan in uitsluitingen
van firewalls, zoals:

*.srvygles.com *.amazonaws.com
*.c-cdsknn.net *.ugwdevice.net

CCA	
hbp-ec1.srvygles.com: poort 443	rgt.srvygles.com: poort 443
kinesis.eu-central-1.amazonaws.com: poort 443	camapi.srvygles.com: poort 443
cognito-identity.eu-central-1.amazonaws.com: poort 443	camapi-ec1.srvygles.com: poort 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com: poort 443 of poort 8883	hbpm-ec1.srvygles.com: poort 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX en nieuwer (standaardmodus)	CDCA v2.XX en nieuwer (CCA-modus)
rgt.srvygles.com	hbp-ec1.srvygles.com
hbpm-ec1.srvygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srvygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srvygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srvygles.com	rgt.srvygles.com
camapis.srvygles.com	hbpm-ec1.srvygles.com
mds-ec1.srvygles.com	camapi-ec1.srvygles.com
gd1p01.c-wss.com	camapis-ec1.srvygles.com
www-ec1.srvygles.com	camapi.srvygles.com
cam-ec1.srvygles.com	camapis.srvygles.com
	mds-ec1.srvygles.com
	gd1p01.c-wss.com
	www-ec1.srvygles.com
	cam-ec1.srvygles.com
Voor RMT, DIAG, MEAP (CCA-modus v4.0 en hoger)	Voor RMT, DIAG, MEAP (HTTP-modus)
hbp-ec1.srvygles.com	a01.ugwdevice.net: poort 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net: poort 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srvygles.com	
hbpm-ec1.srvygles.com	
camapis-ec1.srvygles.com	
camapis.srvygles.com	
camapi-ec1.srvygles.com	
camapi.srvygles.com	
mds-ec1.srvygles.com	
eRDS	
a01.ugwdevice.net: poort 443	
b01.ugwdevice.net: poort 443	
cnvextdata-an1s.srvygles.com: poort 443 is alleen vereist voor externe activering van CCA op bestaande apparaten met eRDS	
Voor RDMS	
device.c-cdsknn.net: poort 443	a02.c-cdsknn.net: poort 443
device02.c-cdsknn.net: poort 443	
Voor Data Backup Service	
hbp-ec1.srvygles.com: poort 443	b01.ugwdevice.net: poort 443
kinesis.eu-central-1.amazonaws.com: poort 443	cnvextdata-an1s.srvygles.com: poort 443
cognito-identity.eu-central-1.amazonaws.com: poort 443	camapi-ec1.srvygles.com: poort 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com: poort 443 of poort 8883	camapis-ec1.srvygles.com: poort 443
rgt.srvygles.com: poort 443	camapi.srvygles.com: poort 443
hbpm-ec1.srvygles.com: poort 443	camapis.srvygles.com: poort 443
a01.ugwdevice.net: poort 443	dcf-ec1.srvygles.com: poort 443

Februari 2025 - V.01



Canon Inc.
canon.com

Canon België / Canon Nederland N.V.
nl.canon.be / www.canon.nl

Dutch edition
© Canon Belgium NV /
© Canon Nederland N.V. 2025

Canon Nederland N.V.
Brabantlaan 2
5216 TV 's-Hertogenbosch
Telefoon: (073) 6 815 815
canon.nl
b2b@canon.nl

Canon Belgium NV
Berkenlaan 3
1831 Diegem
Telefoon: 02 722 04 11
canon.be
contact@canon.be