



**Canon**

# SICUREZZA DELLE INFORMAZIONI CON CANON eMAINTENANCE

Il servizio eMaintenance di Canon gestisce e amministra tutti i dispositivi Canon MFP e SFP connessi alla rete, garantendo il rispetto dei più elevati standard di sicurezza.

# PARTE 1: DOMANDE FREQUENTI

Questo documento è pensato per rispondere alle domande più frequenti relative alla sicurezza di eMaintenance. Per ulteriori informazioni sulla sicurezza di eMaintenance, contatta il tuo rappresentante Canon locale.



## Chi possiede i miei dati?

I tuoi dati sono di tua proprietà. Canon è solo un elaboratore di dati autorizzato per i dati eMaintenance dei clienti.



## Chi può accedere ai miei dati?

---

### Canon adotta un approccio a più livelli per regolamentare l'accesso ai dati, che include:

- **Controlli sull'accesso fisico:** solo le persone autorizzate possono accedere fisicamente ai locali, agli edifici o alle stanze in cui sono conservati i dati personali.
- **Controlli sull'accesso al sistema:** i sistemi che elaborano i dati personali possono essere accessibili solo previa autorizzazione basata sui ruoli degli utenti e sui relativi permessi.
- **Controlli sull'accesso ai dati:** le persone autorizzate ad usare i sistemi di elaborazione dati possono accedere solo ai dati personali a cui hanno diritto.
- **Controlli sulla trasmissione dei dati:** salvo quanto necessario per la fornitura dei servizi, i dati personali non possono essere letti, copiati, modificati o rimossi senza autorizzazione durante il trasferimento.
- **Controlli sull'inserimento dei dati:** Canon implementa misure che consentono di esaminare retrospettivamente e stabilire chi ha inserito, modificato o rimosso i dati personali dai suoi sistemi.

- **Controlli sul lavoro:** tutti i dipendenti Canon e i fornitori di servizi sono contrattualmente obbligati a rispettare la riservatezza delle informazioni sensibili.
- **Controlli sulla separazione dei dati:** i dati personali sono archiviati e accessibili solo dal singolo locatario eMaintenance di ciascun cliente.

### L'accesso ai dati è controllato tramite le seguenti misure:

- Come parte della politica di sicurezza di Canon, i dati personali richiedono almeno lo stesso livello di protezione delle informazioni "riservate".
- L'accesso ai dati personali è concesso solo a chi ne ha bisogno per svolgere il proprio lavoro. Il personale ha accesso alle informazioni necessarie per svolgere le proprie mansioni.
- Le misure di sicurezza per le applicazioni che elaborano i dati personali vengono regolarmente controllate. Canon effettua controlli di sicurezza interni ed esterni e test di penetrazione sui propri sistemi informatici.
- I dati personali non devono essere letti, copiati, modificati o rimossi senza autorizzazione durante l'elaborazione, l'uso e la conservazione.



## I miei dati sono crittografati?

I dati memorizzati nel servizio cloud AWS sono crittografati.

Il trasferimento dei dati tra Canon e i suoi clienti avviene sempre tramite protocolli di trasporto crittografati e sicuri.

I dati personali memorizzati con il servizio opzionale di backup o di assistenza all'installazione, come i dati della rubrica del dispositivo, sono crittografati con AES-256.



## Come vengono separati i miei dati da quelli degli altri clienti?

I dati personali vengono elaborati utilizzando i seguenti controlli di separazione:

Canon utilizza controlli tecnici appropriati per ottenere la separazione logica dei dati del cliente.

Se applicabile, una struttura ad albero multilivello garantisce che un locatario principale possa accedere ai locatari secondari, ma che i locatari secondari non possano accedere ad altri locatari dello stesso livello o di un livello superiore (come quello dei locatari principali).



## Quali dati raccoglie eMaintenance?

La maggior parte dei dati raccolti da eMaintenance sono dati del dispositivo non identificabili personalmente, come nome del cliente, nome del dispositivo, numero di serie, posizione, indirizzo IP, stato e avvisi.

Non vengono raccolte informazioni relative alle operazioni dell'utente, come nome utente, data/ora, nome del documento e contenuto del lavoro (dati immagine/dati di stampa) per COPIA, STAMPA, SCANSIONE e INVIO.



## Canon effettua controlli sulla sicurezza del proprio cloud?

Canon effettua molteplici audit per monitorare lo stato della sicurezza delle informazioni dei servizi cloud che fornisce, garantendo così che Canon e i suoi clienti possano utilizzare i servizi in tutta sicurezza.

Per verificare le misure di sicurezza di eMaintenance, vengono regolarmente effettuati test di penetrazione da parte di terzi.



\* Quando si utilizza il servizio opzionale di backup dei dati o il servizio di assistenza all'installazione, possono essere raccolti dati personali come nome utente e indirizzo e-mail se presenti nella rubrica del dispositivo, ma solo previo specifico accordo con il cliente.



## L'infrastruttura cloud di eMaintenance è sicura?

Il servizio eMaintenance è ospitato sulla piattaforma AWS a Francoforte, in Germania.



## eMaintenance dispone di certificazioni rispetto ai principali standard di sicurezza?

Il Digital Printing Development Center di Canon Inc. è certificato secondo lo standard internazionale ISO/IEC 27001. Questa certificazione riguarda lo sviluppo da parte di Canon Inc. del servizio di monitoraggio (inclusa la suite eMaintenance) per dispositivi multifunzione (MFD) e stampanti.

Con l'ottenimento delle certificazioni ISO/IEC 27001 e ISO/IEC 27017, Canon Inc. conferma che i suoi processi di sicurezza sono certificati da terzi secondo standard internazionali riconosciuti.

Questo dimostra l'impegno di Canon Inc. nella sicurezza delle informazioni, sia all'interno dell'azienda che nell'offerta di servizi online:

- **Riservatezza:** assicurando l'accessibilità delle informazioni solo a personale autorizzato
- **Integrità:** salvaguardando l'accuratezza e l'integrità delle informazioni e dei metodi di elaborazione.
- **Disponibilità:** assicurando l'accessibilità delle informazioni agli utenti autorizzati quando necessario



Lo standard ISO/IEC 27001 richiede revisioni periodiche e garantisce che le funzioni del Servizio di monitoraggio siano sviluppate e fornite da un'organizzazione sicura, certificata da terzi secondo standard internazionali concordati.

Parte di ISO/IEC 27001 include ISO/IEC 27017, che definisce controlli di sicurezza aggiuntivi specifici per i fornitori di servizi cloud. Fornisce un quadro di riferimento per la sicurezza delle informazioni per le organizzazioni che utilizzano servizi cloud.

Canon ha scelto di aderire a questo codice di condotta per garantire ai clienti dei servizi cloud un approccio coerente e completo alla sicurezza delle informazioni.

## LEGENDA

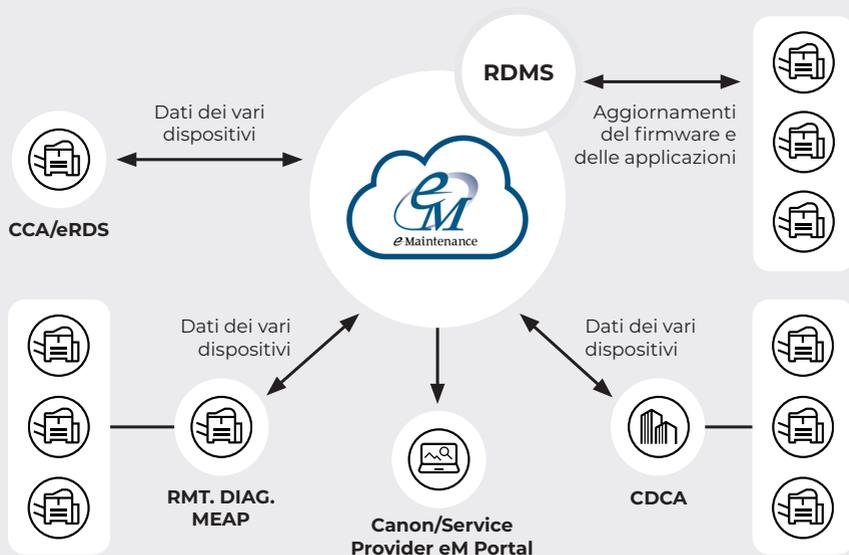
**CCA** - Cloud Connection Agent

**CDCA** - Canon Data Collection Agent

**RMT, DIAG, MEAP** - Remote Diagnostics MEAP

**eRDS** - Embedded Remote Diagnostic System

**RDMS** - Remote Distribution & Management Service



## PARTE 2: REQUISITI DELL'INFRASTRUTTURA eMAINTENANCE

eMaintenance utilizza una serie di agenti locali e applicazioni software per facilitare le comunicazioni tra i dispositivi Canon e il servizio eMaintenance. A seconda del tipo di dispositivo, dell'infrastruttura locale e dei requisiti del servizio, ogni cliente può avere uno o più di questi agenti abilitati.

**Le opzioni sono le seguenti:**

---

### **CCA (Cloud Connection Agent)**

CCA è l'agente integrato più recente per eMaintenance. Funziona internamente sul dispositivo senza la necessità di installare un agente separato per la raccolta dei dati sulla rete. Poiché è in grado di raccogliere una più ampia gamma di dati del dispositivo, la connettività CCA è necessaria per beneficiare di tutte le funzionalità e i servizi più recenti (e futuri) di eMaintenance, inclusa la diagnosi predittiva e la riparazione basata sull'intelligenza artificiale. CCA può essere integrato nei dispositivi esistenti che utilizzano eRDS.

---

### **CDCA (Canon Data Collection Agent)**

CDCA è un agente installato su PC per eMaintenance. Questo software di monitoraggio è installato su un PC locale nella rete del cliente.

---

### **RMT. DIAG. MEAP (Remote Diagnostics MEAP)**

Si tratta di un software agente integrato nel dispositivo per eMaintenance che utilizza la piattaforma MEAP che può essere utilizzato per monitorare il dispositivo host e altri dispositivi Canon sulla rete. È ideale per reti di piccole dimensioni che non richiedono un server CDCA.

---

### **eRDS (embedded Remote Diagnostic Service)**

eRDS è un agente integrato nei dispositivi legacy per eMaintenance. Questo software di monitoraggio funziona internamente al dispositivo. eRDS invia le informazioni di gestione del dispositivo al servizio eMaintenance e può essere configurato per ricevere gli aggiornamenti del firmware e delle licenze delle applicazioni MEAP.

---

### **RDMS (Remote Distribution & Management Service)**

Consente ai provider di servizi Canon autorizzati di gestire prodotti e licenze per le applicazioni MEAP e le opzioni IR, nonché di aggiornare il firmware e le licenze delle applicazioni MEAP.

---

### **Servizio di backup dei dati**

Questo servizio opzionale esegue backup regolari delle impostazioni memorizzate sul dispositivo, in forma crittografata nel cloud. In caso di guasto di HDD/SSD/Controller che richiede una sostituzione, il servizio può ripristinare i dati sul dispositivo riducendo significativamente il tempo di riparazione.

---

### **Accesso alla rete richiesto**

Per permettere il funzionamento di eMaintenance, i clienti devono consentire l'accesso agli URL appropriati attraverso la loro rete per i dispositivi Canon. Rivolgiti al tuo rappresentante Canon per avere l'elenco degli URL specifici necessari per l'ambiente in uso.

# URL DI CONNESSIONE INDIVIDUALE A eMAINTENANCE

Canon raccomanda l'uso di caratteri  
jolly nelle esclusioni del firewall,  
come ad esempio:

\*.srv.ygles.com \*.amazonaws.com  
\*.c-cdsknn.net \*.ugwdevice.net

<b>CCA</b>	
hbp-ec1.srv.ygles.com - Porta 443	rgt.srv.ygles.com - Porta 443
kinesis.eu-central-1.amazonaws.com - Porta 443	camapi.srv.ygles.com - Porta 443
cognito-identity.eu-central-1.amazonaws.com - Porta 443	camapi-ec1.srv.ygles.com - Porta 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Porta 443 or Port 8883	hbpm-ec1.srv.ygles.com - Porta 443
<b>CDCA v1.XX</b>	
b01.ugwdevice.net	
<b>CDCA v2.XX e versioni successive (modalità standard)</b>	<b>CDCA v2.XX e versioni successive (modalità CCA)</b>
rgt.srv.ygles.com	hbp-ec1.srv.ygles.com
hbpm-ec1.srv.ygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ec1.srv.ygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ec1.srv.ygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srv.ygles.com	rgt.srv.ygles.com
camapis.srv.ygles.com	hbpm-ec1.srv.ygles.com
mds-ec1.srv.ygles.com	camapi-ec1.srv.ygles.com
gdlp01.c-wss.com	camapis-ec1.srv.ygles.com
www-ec1.srv.ygles.com	camapi.srv.ygles.com
cam-ec1.srv.ygles.com	camapis.srv.ygles.com
	mds-ec1.srv.ygles.com
	gdlp01.c-wss.com
	www-ec1.srv.ygles.com
	cam-ec1.srv.ygles.com
<b>RMT, DIAG, MEAP (modalità CCA v4.0 e successive)</b>	<b>RMT, DIAG, MEAP (modalità HTTP)</b>
hbp-ec1.srv.ygles.com	a01.ugwdevice.net - Porta 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net - Porta 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srv.ygles.com	
hbpm-ec1.srv.ygles.com	
camapis-ec1.srv.ygles.com	
camapis.srv.ygles.com	
camapi-ec1.srv.ygles.com	
camapi.srv.ygles.com	
mds-ec1.srv.ygles.com	
<b>eRDS</b>	
a01.ugwdevice.net - Porta 443	
b01.ugwdevice.net - Porta 443	
cnvextdata-an1s.srv.ygles.com - La porta 443 è necessaria solo per l'attivazione remota di CCA su dispositivi esistenti con eRDS.	
<b>RDMS</b>	
device.c-cdsknn.net - Porta 443	a02.c-cdsknn.net - Porta 443
device02.c-cdsknn.net - Porta 443	
<b>Per il servizio di backup dei dati</b>	
hbp-ec1.srv.ygles.com - Porta 443	b01.ugwdevice.net - Porta 443
kinesis.eu-central-1.amazonaws.com - Porta 443	cnvextdata-an1s.srv.ygles.com - Porta 443
cognito-identity.eu-central-1.amazonaws.com - Porta 443	camapi-ec1.srv.ygles.com - Porta 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Porta 443 or Port 8883	camapis-ec1.srv.ygles.com - Porta 443
rgt.srv.ygles.com - Porta 443	camapi.srv.ygles.com - Porta 443
hbpm-ec1.srv.ygles.com - Porta 443	camapis.srv.ygles.com - Porta 443
a01.ugwdevice.net - Porta 443	dcf-ec1.srv.ygles.com - Porta 443

Febbraio 2025 - V.01

**Canon Inc.**  
canon.com

**Canon Europe**  
canon-europe.com

**Italian edition /canon.it**  
© Canon Europa N.V. 2025

**Canon Italia Spa**  
Strada Padana Superiore, 2/B  
20063 Cernusco sul Naviglio MI  
Tel 02 82481  
Fax 02 82484600  
Pronto Canon 848800519  
canon.it

**Canon (Svizzera) SA**  
Richtstrasse 9  
CH-8304 Wallisellen  
Tel. +41 (0) 848 833 835  
canon.ch

**Canon**