



Canon

ІНФОРМАЦІЙНА БЕЗПЕКА З CANON eMAINTENANCE

Програма Canon eMaintenance відповідає за контроль і адміністрування всіх ваших мережових БФП- та ОФП-пристроїв Canon із дотриманням суворих протоколів безпеки.

ЧАСТИНА 1. ПОШИРЕНІ ЗАПИТАННЯ

Цей документ має на меті відповісти на основні запитання щодо безпеки, які можуть виникнути у вас стосовно eMaintenance. По додаткову інформацію про засоби захисту, передбачені в eMaintenance, зверніться до місцевого представника Canon.



Кому належать мої дані?

У всіх випадках власником ваших даних є ви, а Canon є лише узгодженим обробником даних eMaintenance клієнтів.



Хто має доступ до моїх даних?

Компанія Canon реалізує багаторівневий підхід до регулювання доступу до даних, зокрема:

- **Контроль фізичного доступу** — право на фізичний доступ до приміщень, будівель або кімнат, де зберігаються персональні дані, мають лише вповноважені особи.
- **Контроль доступу до систем** — доступ до систем, що обробляють персональні дані, можливий лише за умови авторизації на основі ролей користувачів і пов'язаних із ними дозволів.
- **Контроль доступу до даних** — особи, що мають право використовувати системи обробки даних, отримують доступ лише до тих персональних даних, для яких вони мають право доступу.
- **Контроль передавання даних** — за винятком випадків, коли це необхідно для надання послуг згідно з відповідною угодою, персональні дані не можна читати, копіювати, змінювати або видаляти без дозволу під час передавання.
- **Контроль за введенням даних** — Canon вживає заходів, які дають змогу ретроспективно дослідити та встановити, чи були введені, змінені або видалені персональні дані в системах обробки даних Canon, і якщо так, то ким саме.
- **Контроль за виконанням завдань** — усі працівники Canon, а також субпідрядники та інші постачальники послуг за контрактом зобов'язані дотримуватися конфіденційності всієї конфіденційної інформації.
- **Контроль розділення даних** — персональні дані зберігаються та доступні лише з боку окремого орендаря eMaintenance кожного клієнта.

Доступ до даних контролюється за допомогою таких заходів:

- Згідно з політикою безпеки Canon, персональні дані мають щонайменше такий самий рівень захисту, що й «конфіденційна» інформація.
- Доступ до персональних даних надається на основі принципу службової необхідності. Персонал має доступ до інформації, необхідної для виконання безпосередніх обов'язків.
- Заходи безпеки, які забезпечують програми, що обробляють персональні дані, регулярно перевіряються. Із цією метою компанія Canon проводить внутрішні та зовнішні перевірки безпеки й тести на проникнення у свої IT-системи.
- Персональні дані не можна читати, копіювати, змінювати або видаляти без дозволу в процесі оброблення, використання та зберігання.



Чи зашифровані мої дані?

Дані, що зберігаються в хмарному сервісі AWS, зашифровані.

Передавання даних між компанією Canon та її клієнтами завжди здійснюється з використанням захищених транспортних протоколів шифрування.

Особисті дані, які можуть зберігатися під час використання додаткової послуги резервного копіювання даних або послуги підтримки встановлення, наприклад вміст адресної книги пристрою, шифруються на базі алгоритму AES-256.



Як мої дані відокремлюються від даних інших клієнтів?

Персональні дані обробляються із застосуванням таких засобів відокремлення:

Canon використовує відповідні технічні засоби для логічного розділення даних клієнтів.

Там, де це можливо, багаторівнева деревоподібна структура забезпечує доступ батьківського орендаря до відповідних дочірніх орендарів, однак дочірні вузли не мають доступу до інших орендарів того ж або вищого рівня (наприклад, до батьківських вузлів).



Які дані збирає система eMaintenance?

Більшість відомостей, які збирає та використовує eMaintenance, — це неперсоніфіковані дані про пристрій, як-от клієнт, назва пристрою, серійний номер, місцезнаходження, IP-адреса, стан та сповіщення.

eMaintenance не збирає такі відомості: інформацію, пов'язану з роботою користувача, наприклад ім'я користувача*, дата й час, назва документа, вміст завдання (дані зображення/друку) для КОПІЮВАННЯ, ДРУКУ, СКАНУВАННЯ та НАДСИЛАННЯ.



Чи проводить Canon аудит хмарної безпеки?

Компанія Canon проводить різноманітні види аудиту, що є індикаторами стану впровадження інформаційної безпеки хмарних сервісів, які вона надає, щоб гарантувати, що компанія Canon та її клієнти можуть користуватися цими сервісами з впевненістю.

Для перевірки заходів безпеки eMaintenance третя сторона регулярно проводить тести на проникнення.

* Під час використання опціональних послуг резервного копіювання даних або підтримки встановлення можуть збиратися особисті дані, такі як ім'я користувача та адреса електронної пошти, якщо вони містяться в адресній книзі пристрою, але лише за спеціальною домовленістю з клієнтом.





Чи захищена хмарна інфраструктура eMaintenance?

Сервіс eMaintenance розміщено на платформі AWS, розташованій у Франкфурті, Німеччина.



Чи має eMaintenance сертифікат відповідності основним стандартам безпеки?

Центр розвитку цифрового друку компанії Canon Inc. сертифікований відповідно до міжнародного стандарту ISO/IEC 27001. Отриманий сертифікат пов'язаний із розробкою компанією Canon Inc. служби моніторингу (включно з eMaintenance Suite) для багатofункціональних пристроїв (БФП) і принтерів.

Отримавши сертифікати ISO/IEC 27001 та ISO/IEC 27017, компанія Canon Inc. може підтвердити, що її процеси безпеки були сертифіковані третьою стороною на відповідність міжнародно визнаним стандартам.

Цей стандарт демонструє прихильність Canon Inc. до інформаційної безпеки всередині компанії та в наших службах онлайн:

- **Конфіденційність** — забезпечення доступу до інформації лише тим особам, хто має на це право.
- **Цілісність** — захист точності й повноти інформації та методів її оброблення.



- **Доступність** — забезпечення доступу авторизованих користувачів до інформації в разі потреби.

ISO/IEC 27001 вимагає регулярного перегляду й означає, що функції служби моніторингу розробляються й надаються надійною та безпечною організацією, що підтверджено незалежною сертифікацією відповідно до узгоджених міжнародних стандартів.

Частиною ISO/IEC 27001 є стандарт ISO/IEC 27017, який визначає додаткові засоби контролю безпеки спеціально для постачальників хмарних послуг. Він окреслює межі інформаційної безпеки для організацій, що використовують хмарні сервіси.

Компанія Canon вирішила дотримуватися цього стандарту, оскільки він захищає її клієнтів хмарних сервісів, забезпечуючи послідовний і комплексний підхід до інформаційної безпеки.

ОСНОВНЕ

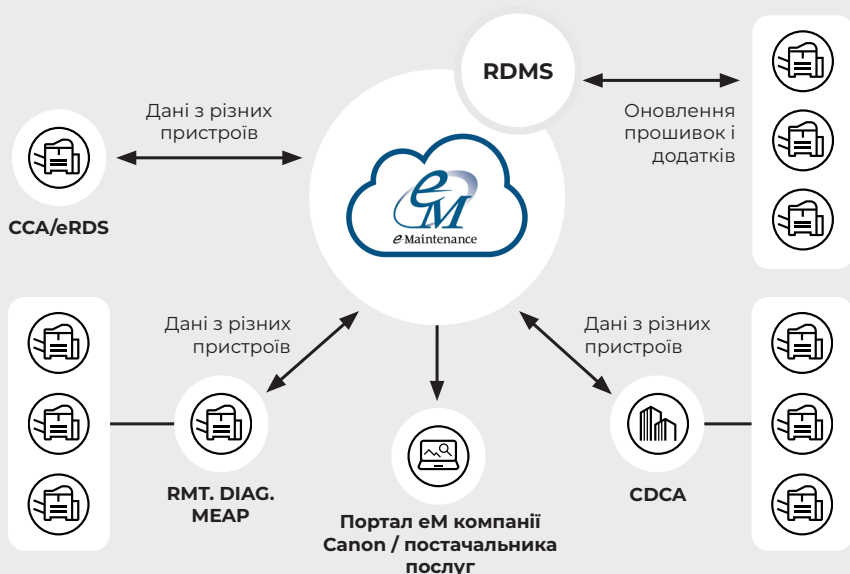
CCA — Cloud Connection Agent, агент підключення до хмари

CDCA — Canon Data Collection Agent, агент збирання даних Canon

RMT. DIAG. MEAP — MEAP віддаленої діагностики

eRDS — embedded Remote Diagnostic System, вбудована система віддаленої діагностики

RDMS — Remote Distribution & Management Service, служба віддаленого розподілу та керування



ЧАСТИНА 2. ВИМОГИ ДО ІНФРАСТРУКТУРИ eM

eM використовує низку локальних агентів та програмних додатків для забезпечення зв'язку між пристроями Canon і сервісом eM. Залежно від певних факторів, таких як тип пристрою, налаштування локальної інфраструктури та вимоги до послуг, у кожного клієнта може бути увімкнено один або кілька із цих агентів.

Доступні такі опції:

CCA (Cloud Connection Agent, агент підключення до хмари)

CCA — це новітній вбудований агент eMaintenance, який працює на пристрої без установлення окремого агента для збирання даних у мережі. Оскільки він може збирати ширший спектр інформації про пристрої, підключення CCA необхідне для використання всіх новітніх (і майбутніх) функціональних можливостей і послуг eMaintenance, включно з предиктивною діагностикою та ремонтом на основі штучного інтелекту. CCA можна додати до наявних пристроїв, на яких працює eRDS.

CDCA (Canon Data Collection Agent, агент збирання даних Canon)

Це встановлений на ПК агент для eMaintenance. Це програмне забезпечення для моніторингу встановлюється на локальний ПК в мережі клієнта.

RMT. DIAG. MEAP (дистанційна діагностика MEAP)

Це вбудоване в пристрій програмне забезпечення агента для eMaintenance із застосуванням платформи MEAP, яке можна використовувати для моніторингу головного пристрою та інших пристроїв Canon у мережі. Ідеально підходить для невеликих мереж, які не потребують сервера CDCA.

eRDS (embedded Remote Diagnostic System, вбудована система віддаленої діагностики)

eRDS — це вбудований агент eMaintenance для застарілих пристроїв. Це програмне забезпечення для моніторингу працює всередині самого пристрою. eRDS надсилає інформацію для керування пристроєм до служби eMaintenance і може бути налаштований для отримання оновлень прошивки та ліцензій додатків MEAP.

RDMS (Remote Distribution & Management Service, служба віддаленого розподілу та керування)

Дає змогу авторизованим постачальникам послуг Canon керувати продуктами та ліцензіями для додатків MEAP та опцій iR, а також оновлювати прошивку та ліцензії для додатків MEAP.

Послуга резервного копіювання даних

Ця додаткова послуга забезпечує регулярне заплановане резервне копіювання налаштувань, що зберігаються на внутрішньому накопичувачі, у зашифрованому вигляді до хмарного сховища. У разі виходу з ладу HDD/SSD/контролера з необхідністю його заміни послуга резервного копіювання даних може відновити дані на пристрої, значно скоротивши час ремонту.

Необхідний доступ до мережі

Для використання функцій eMaintenance клієнтам буде запропоновано надати пристроям Canon доступ до відповідних URL-адрес через їхню мережу. За списком конкретних URL-адрес, необхідних для вашого середовища, зверніться до свого представника Canon.

ОКРЕМІ URL-АДРЕСИ ДЛЯ ПІДКЛЮЧЕННЯ ДО eMAINTENANCE

Canon рекомендує використовувати символи підстановки у винятках брендмауера, як-от:

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

ССА	
hbp-ecl.srvygles.com — порт 443	rgt.srvygles.com — порт 443
kinesis.eu-central-1.amazonaws.com — порт 443	camapi.srvygles.com — порт 443
cognito-identity.eu-central-1.amazonaws.com — порт 443	camapi-ecl.srvygles.com — порт 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com — порт 443 або порт 8883	hbpm-ecl.srvygles.com — порт 443
CDCA 1.XX	
b01.ugwdevice.net	
CDCA 2.XX та новіші версії (стандартний режим)	CDCA 2.XX та новіші версії (режим ССА)
rgt.srvygles.com	hbp-ecl.srvygles.com
hbpm-ecl.srvygles.com	kinesis.eu-central-1.amazonaws.com
camapi-ecl.srvygles.com	cognito-identity.eu-central-1.amazonaws.com
camapis-ecl.srvygles.com	a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com
camapi.srvygles.com	rgt.srvygles.com
camapis.srvygles.com	hbpm-ecl.srvygles.com
mds-ecl.srvygles.com	camapi-ecl.srvygles.com
gdlp01.c-wss.com	camapis-ecl.srvygles.com
www-ecl.srvygles.com	camapi.srvygles.com
cam-ecl.srvygles.com	camapis.srvygles.com
	mds-ecl.srvygles.com
	gdlp01.c-wss.com
	www-ecl.srvygles.com
	cam-ecl.srvygles.com
Для RMT, DIAG, MEAP (режим ССА 4.0 і новіші версії)	Для RMT, DIAG, MEAP (режим HTTP)
hbp-ecl.srvygles.com	a01.ugwdevice.net — порт 443
kinesis.eu-central-1.amazonaws.com	b01.ugwdevice.net — порт 443
cognito-identity.eu-central-1.amazonaws.com	
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com	
rgt.srvygles.com	
hbpm-ecl.srvygles.com	
camapis-ecl.srvygles.com	
camapis.srvygles.com	
camapi-ecl.srvygles.com	
camapi.srvygles.com	
mds-ecl.srvygles.com	
eRDS	
a01.ugwdevice.net — порт 443	
b01.ugwdevice.net — порт 443	
cnvextdata-anls.srvygles.com — порт 443 потрібен лише для віддаленої активації ССА на наявних пристроях з eRDS	
Для RDMS	
device.c-cdsknn.net — порт 443	a02.c-cdsknn.net — порт 443
device02.c-cdsknn.net — порт 443	
Для служби резервного копіювання даних	
hbp-ecl.srvygles.com — порт 443	b01.ugwdevice.net — порт 443
kinesis.eu-central-1.amazonaws.com — порт 443	cnvextdata-anls.srvygles.com — порт 443
cognito-identity.eu-central-1.amazonaws.com — порт 443	camapi-ecl.srvygles.com — порт 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com — порт 443 або порт 8883	camapis-ecl.srvygles.com — порт 443
rgt.srvygles.com — порт 443	camapi.srvygles.com — порт 443
hbpm-ecl.srvygles.com — порт 443	camapis.srvygles.com — порт 443
a01.ugwdevice.net — порт 443	dcf-ecl.srvygles.com — порт 443

Лютий 2025 р., версія 01



Canon Inc.
canon.com

Canon Europe
canon-europe.com

Ukrainian edition
© Canon Europa N.V., 2025.

ТОВ «Кенон Україна»
01601, Київ, ул. Мечникова, 2А
Україна
Телефон: +38 044 490 2595
Факс: +38 044 490 2598
www.canon.ua