



Canon

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ С CANON eMAINTENANCE

Решение Canon eMaintenance возьмет на себя задачи управления и администрирования всем парком ваших сетевых МФУ и однофункциональных устройств Canon согласно строжайшим протоколам безопасности.

ЧАСТЬ 1. ЧАСТО ЗАДАВАЕМЫЕ ВОПРОСЫ

Этот документ поможет вам найти ответы на основные вопросы по безопасности относительно eMaintenance. Больше сведений о средствах безопасности, встроенных в eMaintenance, вы можете получить у местного представителя Canon.



Кто владеет моими данными?

В любых ситуациях использования ваши данные принадлежат только вам, а Canon является доверенным обработчиком клиентских данных eMaintenance.



Кто может осуществлять доступ к моим данным?

Canon предлагает многоуровневый подход к управлению доступом к данным, включая:

- **Физические средства контроля доступа:** только авторизованный персонал имеет физический доступ к офисам, сооружениям и помещениям, где хранятся персональные данные.
- **Средства контроля доступа через систему:** системы обработки персональных данных можно открыть только после авторизации пользователей на основании их ролей и связанных уровней доступа.
- **Средства контроля доступа к данным:** лица с разрешением на использование систем обработки данных получают доступ только к определенным данным, а не ко всей системе.
- **Средства управления передачей данных:** за исключением ситуаций, где это необходимо для предоставления услуг согласно условиям соглашения, чтение, копирование, изменение и удаление персональных данных при передаче не осуществляется без соответствующего уровня авторизации.
- **Средства управления вводом данных:** Canon внедряет меры, которые позволяют ретроспективно изучать персональные данные на предмет того, осуществлялся ли, а также кем осуществлялся их ввод, изменение или удаление из систем обработки данных Canon.

- **Средства управления заданиями:** все сотрудники Canon, связанные контрактом субобработчики и прочие поставщики услуг согласно контракту обязуются сохранять конфиденциальность всей информации, не подлежащей разглашению.
- **Средства разделения данных:** персональные данные хранятся и открываются только через отдельный профиль eMaintenance каждого клиента.

Доступ к данным осуществляется при управлении с помощью следующих мер:

- Согласно Политике безопасности Canon, персональным данным требуется такой же уровень защиты, как и конфиденциальной информации.
- Доступ к персональным данным осуществляется только на основе необходимости использования конкретных сведений. У персонала есть доступ к информации, которая им необходима для выполнения своих рабочих обязанностей.
- Меры по безопасности, которые защищают приложения для обработки персональных данных, регулярно проверяются на актуальность. Для этого Canon выполняет внутренние и внешние проверки безопасности, а также проводит испытания на проникновение для своих ИТ-систем.
- Персональные данные не должны подлежать чтению, копированию, изменению или удалению без соответствующей авторизации в рамках их обработки, использования и хранения.



Мои данные шифруются?

Данные, которые хранятся в облачном сервисе AWS, шифруются.

Когда данные передаются между Canon и нашими клиентами, такие операции всегда производятся с использованием безопасных протоколов шифрования при передаче.

Персональные данные, которые могут храниться с использованием опциональной службы резервного копирования данных или службы поддержки при установке, например данные адресной книги устройства, шифруются по протоколу AES-256.



Как мои данные отделяются от данных других клиентов?

Персональные данные обрабатываются с использованием следующих инструментов разделения:

Canon использует соответствующие технические инструменты контроля для достижения логического разделения клиентских данных.

Где это применимо, многоуровневая древообразная структура обеспечивает доступ ведущего профиля к подчиненному, однако подчиненные профили не имеют доступа к другим профилям того же или более высокого уровня (например, к ведущему профилю).



Какие данные собираются eMaintenance?

Большая часть данных, которые собирает eMaintenance, — это данные с устройства, не позволяющие идентифицировать личность пользователя, такие как имя клиента, название устройства, серийный номер, местоположение, IP-адрес, состояние и оповещения.

Следующие сведения не собираются eMaintenance: информация, связанная с действиями пользователя, такая как имя пользователя*, название документа, а также содержимое заданий (данные изображения и данные для печати) для функций КОПИРОВАНИЯ, ПЕЧАТИ, СКАНИРОВАНИЯ и ОТПРАВКИ.



Проводит ли Canon аудит своей облачной безопасности?

Canon проводит различные аудиты и использует их для оценки внедрения службы информационной безопасности в предоставляемых облачных сервисах — все для того, чтобы и Canon, и клиенты компании могли быть уверены в безопасной работе таких систем.

Для подтверждения эффективности мер обеспечения безопасности eMaintenance мы регулярно организуем испытания на проникновение с участием третьих лиц.

*При использовании персональных данных, связанных с опциональными службами резервного копирования данных и поддержки при установке, такие сведения, как имя пользователя и адрес электронной почты могут собираться, если содержатся в адресной книге устройства, однако только при условии отдельного соглашения с клиентом.





Безопасна ли облачная инфраструктура eMaintenance?

Служба eMaintenance располагается на платформе AWS во Франкфурте, Германия.



Есть ли у eMaintenance какие-либо сертификаты соответствия основным стандартам безопасности?

Центр разработок цифровой печати Canon Inc. сертифицирован на соответствие международному стандарту ISO/IEC 27001. Эта сертификация получена в отношении разработки Canon Inc. службы мониторинга (включая eMaintenance Suite) для многофункциональных устройств (МФУ) и принтеров.

Получение ISO/IEC 27001 и ISO/IEC 27017 означает, что в Canon Inc. используются процессы обеспечения безопасности, протестированные независимой организацией и соответствующие международным стандартам качества.

Этот стандарт демонстрирует стремление Canon Inc. к информационной безопасности внутри компании и нашего ассортимента онлайн-сервисов:

- **Конфиденциальность** — предоставление доступа к информации только лицам, имеющим право на доступ к ней.
- **Целостность** — обеспечение точности и полноты информации и методов обработки.
- **Доступность** — обеспечение доступа авторизованных пользователей к информации при необходимости.



ISO/IEC 27001 требует регулярного проведения проверок и означает, что функции службы мониторинга разрабатываются и развертываются безопасной и защищенной организацией — это подтверждает сторонняя сертификация на соответствие утвержденным международным стандартам.

Часть ISO/IEC 27001 включает ISO/IEC 27017, которая определяет дополнительные меры управления безопасностью специально для поставщиков облачных сервисов. Он содержит основные требования к информационной безопасности для организаций, использующих облачные сервисы.

Canon соответствует требованиям этой сертификации в отношении управления информационной безопасностью, поскольку это обеспечивает безопасность клиентов наших облачных сервисов и создает стабильную, комплексную практику в отношении информационной безопасности.

АББРЕВИАТУРЫ

CCA - Cloud Connection Agent

CDCA - Canon Data Collection Agent

RMT. DIAG. MEAP - MEAP удаленной диагностики

eRDS - Встроенная система удаленной диагностики

RDMS - Служба удаленного распределения и управления



ЧАСТЬ 2. ТРЕБОВАНИЯ К ИНФРАСТРУКТУРЕ eM

eM использует большое количество логических агентов и программных приложений для обеспечения коммуникации между устройствами Canon и сервисов eM. В зависимости от ряда факторов, таких как тип устройства, конфигурация локальной инфраструктуры и требования к сервису, каждый клиент может включить или отключить любой из них.

Доступные опции:

CCA (Cloud Connection Agent)

CCA — это новейший встроенный агент устройства для eMaintenance, который работает на устройстве без необходимости в установке внутри сети отдельного агента для сбора данных. CCA может собирать широкий спектр данных устройства, поэтому подключение CCA требуется для использования всех текущих и будущих функциональных преимуществ сервиса eMaintenance, включая предиктивную диагностику и ремонт с помощью ИИ. CCA можно добавить на уже имеющиеся устройства с eRDS.

CDCA (Canon Data Collection Agent)

Это агент для eMaintenance, который устанавливается на ПК. Это ПО для мониторинга устанавливается на ПК, подключенный к клиентской сети.

RMT. DIAG. MEAP (MEAP удаленной диагностики)

Это встроенное в устройство ПО-агент для eMaintenance на базе платформы MEAP, которую можно использовать для мониторинга хост-устройства и прочих устройств Canon в сети. Идеально для небольших сетей, где не требуется установка сервера CDCA.

eRDS (Встроенная система удаленной диагностики)

eRDS — это старый встроенный в устройство агент для eMaintenance. Это ПО для мониторинга самостоятельно работает внутри устройства. eRDS отправляет сведения об управлении устройством в службу eMaintenance, и его можно настроить на получение лицензионных обновлений для встроенного ПО и приложения MEAP.

RDMS (Служба удаленного распределения и управления)

Позволяет авторизованным поставщикам служб Canon управлять продуктами и лицензиями для приложений MEAP и опций iR, а также развертывать лицензии и обновления встроенного ПО и MEAP.

Служба резервного копирования данных

Эта опциональная служба регулярно осуществляет резервное копирование настроек, сохраненных во внутренней памяти устройства, и в зашифрованном виде отправляет их в облако на хранение. В случае сбоя жесткого диска, SSD-накопителя или контроллера и необходимости их замены служба резервного копирования данных позволит избежать утери данных и восстановить их на новом устройстве для минимального времени простоя.

Требуемый сетевой доступ

Для активации функций eMaintenance клиентам потребуется предоставить устройствам Canon в своей сети доступ к ряду URL-адресов. Запросите актуальный список URL-адресов под вашу сетевую среду у своего представителя Canon.

ИНДИВИДУАЛЬНЫЕ URL-АДРЕСА ПОДКЛЮЧЕНИЯ ДЛЯ eMAINTENANCE

Canon рекомендует использовать wildcard-сертификаты в исключениях Firewall, таких как:

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

ССА	
hbp-ec1.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-ec1.srvygles.com - Порт 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Порт 443 ali Порт 8883	hbpm-ec1.srvygles.com - Порт 443
CDCA v1.XX	
b01.ugwdevice.net	
CDCA v2.XX и новее (стандартный режим)	CDCA v2.XX и новее (режим ССА)
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
gdlp01.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
	gdlp01.c-wss.com
	www-ec1.srvygles.com
	cam-ec1.srvygles.com
Для RMT, DIAG, MEAP (режим ССА v4.0 и выше)	Для RMT, DIAG, MEAP (режим HTTP)
hbp-ec1.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-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 - Порт 443	
b01.ugwdevice.net - Порт 443	
cnvextdata-anls.srvygles.com - Порт 443 требуется только для удаленной активации ССА на текущих устройствах с eRDS	
Для RDMS	
device.c-cdsknn.net - Порт 443	a02.c-cdsknn.net - Порт 443
device02.c-cdsknn.net - Порт 443	
Для службы резервного копирования данных	
hbp-ec1.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-ec1.srvygles.com - Порт 443
a2etju7iemltgc-ats.iot.eu-central-1.amazonaws.com - Порт 443 или 8883	camapis-ec1.srvygles.com - Порт 443
rgt.srvygles.com - Порт 443	camapi.srvygles.com - Порт 443
hbpm-ec1.srvygles.com - Порт 443	camapis.srvygles.com - Порт 443
a01.ugwdevice.net - Порт 443	dcf-ec1.srvygles.com - Порт 443

Февраль 2025 года - V.01



Canon Inc.
canon.com

Canon Europe
canon-europe.com

Russian edition
© Canon Europa N.V. 2025

Canon CEE GMBH
Am Europlatz 2
A-1120 Vienna
Austria