?????????? ??????? ?????

Зона ответственности: Printum + Заказчик / Интегратор

Коротко: Printum поддерживает передачу данных по защищённым каналам связи с использованием HTTPS, TLS и IPPS. Конкретный уровень защиты определяется используемыми сертификатами и настройками инфраструктуры.

??????????

Передаваемые данные должны быть защищены от перехвата, изменения и подмены в процессе передачи по сети.

Использование защищённых каналов связи обеспечивает конфиденциальность и целостность данных при взаимодействии пользователей, компонентов системы и внешних сервисов.

??? ??? ???????????? ? Printum

Для защиты данных при передаче Printum поддерживает использование защищённых сетевых соединений.

В зависимости от сценария эксплуатации могут использоваться:

- HTTPS для взаимодействия пользователей с веб-интерфейсами системы;
- TLS для взаимодействия с внешними сервисами и интеграциями;
- IPPS для защищённой печати по сети.

При использовании защищённых соединений обеспечиваются:

- шифрование передаваемых данных;
- контроль целостности данных;
- проверка подлинности удалённого узла на основе сертификатов.

Пользовательские интерфейсы системы работают через веб-сервер Nginx и поддерживают использование HTTPS.

Поддерживается HTTP/2.

Для повышения безопасности веб-сессий используются защищённые cookie-файлы и механизмы защиты веб-приложений, включая ограничения SameSite для cookie и защиту от встраивания страниц в сторонние сайты.

Printum поддерживает работу за обратными прокси-серверами и балансировщиками нагрузки, передающими информацию о защищённом соединении через стандартные HTTP-заголовки.

Printum поддерживает использование сертификатов, выпущенных корпоративным удостоверяющим центром, доверенным центром сертификации или созданных самостоятельно в соответствии с требованиями организации.

Подробная информация о сертификатах приведена в статье «Управление сертификатами (PKI / CA)».

??? ?????????? ?? ??????????????

Настройка сертификатов, параметров TLS и политик сетевой безопасности выполняется администраторами инфраструктуры заказчика.

При использовании корпоративной инфраструктуры открытых ключей выпуск, продление и отзыв сертификатов выполняются средствами удостоверяющего центра организации.

Revision #1
Created 2026-06-08 19:39:13 UTC by DD
Updated 2026-06-08 19:39:13 UTC by DD