

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

????????????? ??? ??????????????,
?? ? ?????????? ??

???????????

При установке системы автоматически создаётся самоподписанный SSL-сертификат, стандарта SHA-256 с длиной ключа шифрования RSA 2048 бит. Для работы мониторинга и управления печать в сети организации этого достаточно, но при необходимости (например, требования ИБ) допускается установка доверенного сертификата организации.

При необходимости используйте доверенный сертификат одного из типов:

- Сертификат, приобретённый или полученный у внешнего доверенного центра сертификации.
- Сертификат, выданный внутренним центром сертификации организации (Enterprise CA).

????????? HTTPS

Клиент ПринтМенеджера, отправляющий задания на печать с ПК пользователей, имеет параметр `verify_SSL_cert`, отвечающий за включение проверки сертификата безопасности. По умолчанию параметр установлен в `false`, т.е. проверка отключена.

Для включения проверки и обеспечения шифрованного соединения клиента ПМ с сервером ПринтМенеджера выполните настройки, описанные в разделах ниже, в соответствии с операционной системой на пользовательском АРМ.

????????? ?????????? HTTPS-?????????????? ??? ??????? ? Linux

Для корректной проверки сертификата и работы Клиента ПринтМенеджер по протоколу HTTPS выполните следующие действия:

1. Остановите службу Клиента ПМ:

```
sudo systemctl stop printum-printmanager-client.service
```

2. Откройте файл корневого сертификата, который подтверждает подлинность SSL-сертификата, используемого сервером ПМ. Скопируйте из него весь текст, вместе с `BEGIN`, `END` и дефисами.
3. Откройте с правами на редактирование файл:

```
/opt/printum/printmanager_client/venv/lib/python3.10/site-packages/certifi/cacert.pem
```

Для более ранних версий службы для Linux замените `python3.10` на `python3.8`.

4. В конец файла вставьте скопированное из шага 2 и сохраните файл.
5. Запустите службу Клиента ПМ:

```
sudo systemctl start printum-printmanager-client.service
```

????????? ???????? HTTPS-????????????? ??? ?????? ? Windows

1. Откройте файл корневого сертификата, который подтверждает подлинность SSL-сертификата, используемого сервером ПМ. Скопируйте из него весь текст, вместе с `BEGIN`, `END` и дефисами.
2. Откройте с правами на редактирование файл:

```
C:\Program Files\printum\printmanager_client\lib\certifi\cacert.pem
```

3. В конец файла вставьте скопированное из шага 1 и сохраните файл.
4. Перезапустите службу или перезагрузите компьютер.

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

Данные между пользователем и системой, а также между компонентами (Мониторинг и ПринтМенеджер) передаются по протоколу HTTPS.

Тип пароля	Метод	Описание
------------	-------	----------

Пользовательские пароли (вход в систему)	PBKDF2	Хэширование с уникальной «солью» и несколькими десятками итераций
Пароли принтеров, доступа к каталогам и др.	AES CBC 128-bit + PKCS7	Шифрование с 128-битным ключом

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

- [Настройка IPPS для МФУ](#)
 - [Обновление сертификатов Мониторинга и ПринтМенеджера](#)
 - [Переменные .env Мониторинга](#)
-