????????? SSL ??? ????? ???????????

??????????

При установке системы автоматически создаётся самоподписанный SSL-сертификат. Для работы в сети организации это, как правило, не создаёт проблем. Однако в ряде случаев (доступ через интернет, требования ИБ) может потребоваться установка доверенного сертификата.

Для шифрования используются сертификаты стандарта SHA-256 с шифрованием RSA 2048 бит. Пароли не хранятся и не передаются по сети в открытом виде.

????????? HTTPS

Клиентская служба ПринтМенеджера, отправляющая задания на печать с ПК пользователей, имеет параметр `verify_SSL_cert`, по умолчанию установленный в `false`.

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).

Важно: для использования встраиваемого приложения настройка HTTPS может быть обязательной для конкретного вендора. При этом сертификат не обязательно должен быть доверенным. Подробнее — в документации по установке встраиваемых приложений.

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

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

1. Остановите службу Клиента ПМ:

```
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. Перезапустите службу или перезагрузите компьютер.

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

Revision #9
Created 2026-05-10 17:37:53 UTC by DD
Updated 2026-06-14 19:00:44 UTC by DD