# Руководство по настройке хранения секретов служб в отдельной БД

Службы Оркестратора:

1. WebApi
2. RobotLogs
3. States
4. Notifications

могут хранить свои секреты в отдельной БД ltoolssecrets. Для этого требуется:

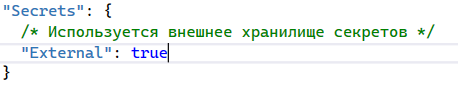
1. Установить переменную окружения SecretsConnection со строкой подключения к БД с секретами ltoolssecrets (пароль в строке подключения должен быть зашифрован[[1]](#footnote-1)):

PORT=5432;TIMEOUT=15;POOLING=True;MINPOOLSIZE=1;MAXPOOLSIZE=20;COMMANDTIMEOUT=20;DATABASE=ltoolssecrets;HOST=192.168.1.172;USER ID=postgres;PASSWORD= 49EqQ30zfcQTWxEGYE/mSw==

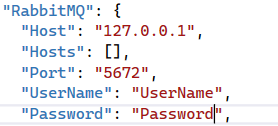
2. При запуске служб Оркестратора БД с секретами создастся автоматически, все пароли будут иметь стандартные значения в незашифрованном виде. Эти пароли нужно будет заменить своими и зашифровать. Секреты хранятся в таблицах:

|  |  |  |  |
| --- | --- | --- | --- |
| №  п/п | Служба | Таблица | Примечание |
|  | WebApi | WebApi | В виде пар ключ-значение[[2]](#footnote-2) |
|  | WebApiAD | Секреты из секции ActiveDirectory: MultyForest для каждого AD |
|  | WebApiTenantIncomingEmail | Секреты из секции Tenants:Items для IncomingEmail каждого недефолтного тенанта |
|  | RobotLogs | RobotLogs | В виде пар ключ-значение |
|  | States | States | В виде пар ключ-значение |
|  | Notifications | Notifications | В виде пар ключ-значение |

3. В конфигурационный файл служб[[3]](#footnote-3) добавить (если отсутствует) секцию Secrets с параметром External = true и перезапустить службу:



4. В конфигурационном файле заменить секреты на заглушки. Например,



1. Здесь и далее пароли шифруются при помощи LTools.Orchestrator.PasswordEncriptor [↑](#footnote-ref-1)
2. На основе одноименной иерархии в конфигурационном файле. Например, RabbitMQ:UserName [↑](#footnote-ref-2)
3. appsettings.ProdWin.json или appsettings.ProdLinux.json [↑](#footnote-ref-3)