



Бастион-3 – Хранилище секретов. Руководство администратора

Версия 2025.4

(17 апреля, 2026)



Самара, 2026



Содержание

1.	Общие сведения.....	4
1.1.	Назначение и область применения.....	4
1.2.	Условия применения.....	4
2.	Настройка системы	5
2.1.	Общие сведения.....	5
2.2.	Настройка подключения к хранилищу секретов	5
2.2.1.	Настройка с помощью приложения «Локальные настройки»	5
2.2.2.	Настройка с помощью консольной утилиты VCSnfg	8
2.3.	Настройка путей к секретам в хранилище	10
3.	Приложения.....	12
3.1.	Приложение 1. Список секретов	12



1. Общие сведения

1.1. Назначение и область применения

Модуль «Бастиян-3 – Хранилище секретов» предназначен для интеграции ПК «Бастиян-3» с системами хранения секретов на основе HashiCorp Vault.

При использовании этого модуля все секреты ПК «Бастиян-3» будут храниться в отдельном специализированном хранилище. В БД ПК «Бастиян-3» и файлах локальных настроек вместо значений секретов хранятся пути для получения значений секретов из хранилища.

К секретам ПК «Бастиян-3» относятся все виды информации, позволяющие аутентифицироваться или авторизоваться для выполнения определённых действий в системе. Конкретно, это могут быть:

1. Сертификаты TLS.
2. Токены API.
3. Пароли.
4. Ключи шифрования.

При использовании модуля «Бастиян-3 – Хранилище секретов», ПК «Бастиян-3» только получает информацию о секретах, но не управляет ей. Таким образом, при применении внешнего хранилища секретов можно организовать централизованное управление секретами на основе корпоративных стандартов. Например, можно централизованно перевыпускать сертификаты и управлять процессом смены паролей.

1.2. Условия применения

Для работы модуля «Бастиян-3 – Хранилище секретов» требуется отдельная серверная лицензия. Модуль совместим с исполнениями сервера «Стандартный» и «Корпоративный».

Лицензия на модуль проверяется после подключения к серверу системы. Если интеграция с хранилищем секретов была включена при отсутствии лицензии, то клиенты будут останавливать свою работу после получения информации, необходимой для подключения к серверу системы.

Для работы модуля требуется подключение к HashiCorp Vault или аналогичной системе с тем же программным интерфейсом. Описание установки и настройки систем хранения секретов выходят за рамки этого руководства.

2. Настройка системы

2.1. Общие сведения

Для активации интеграции с хранилищем секретов требуется выполнить следующие шаги:

1. Настроить параметры соединения с сервером хранилища секретов.
2. Настроить способы получения секретов и их расположения, для каждого секрета отдельно.

Настройка подключения к хранилищу секретов производится на каждом компьютере, где требуется получать секреты из хранилища, отдельно.

Настройку можно выполнить с помощью приложения «Локальные настройки» или через интерфейс командной строки `Vsnfg`.



Внимание!

Секреты необходимо получать только на серверах системы и оборудования. Поэтому, настраивать интеграцию с хранилищем секретов нужно только на серверах. На клиентских рабочих местах, где выполняются только пользовательские приложения системы, никаких настроек производить не требуется.

2.2. Настройка подключения к хранилищу секретов

2.2.1. Настройка с помощью приложения «Локальные настройки»

Настройка производится на странице «Хранилище секретов» (Рис. 1).

Для включения интеграции следует установить флаг «Включить интеграцию с хранилищем секретов».



Внимание!

Система не производит запись данных в хранилище секретов ни при каких условиях. Поэтому, все секреты должны быть предварительно настроены в хранилище. Список секретов см. в Приложении 1. В момент включения интеграции с хранилищем секретов никакие секреты, хранимые до этого в БД ПК «Бастион-3», не удаляются. После включения интеграции необходимо для каждого секрета указать его расположение в хранилище секретов.

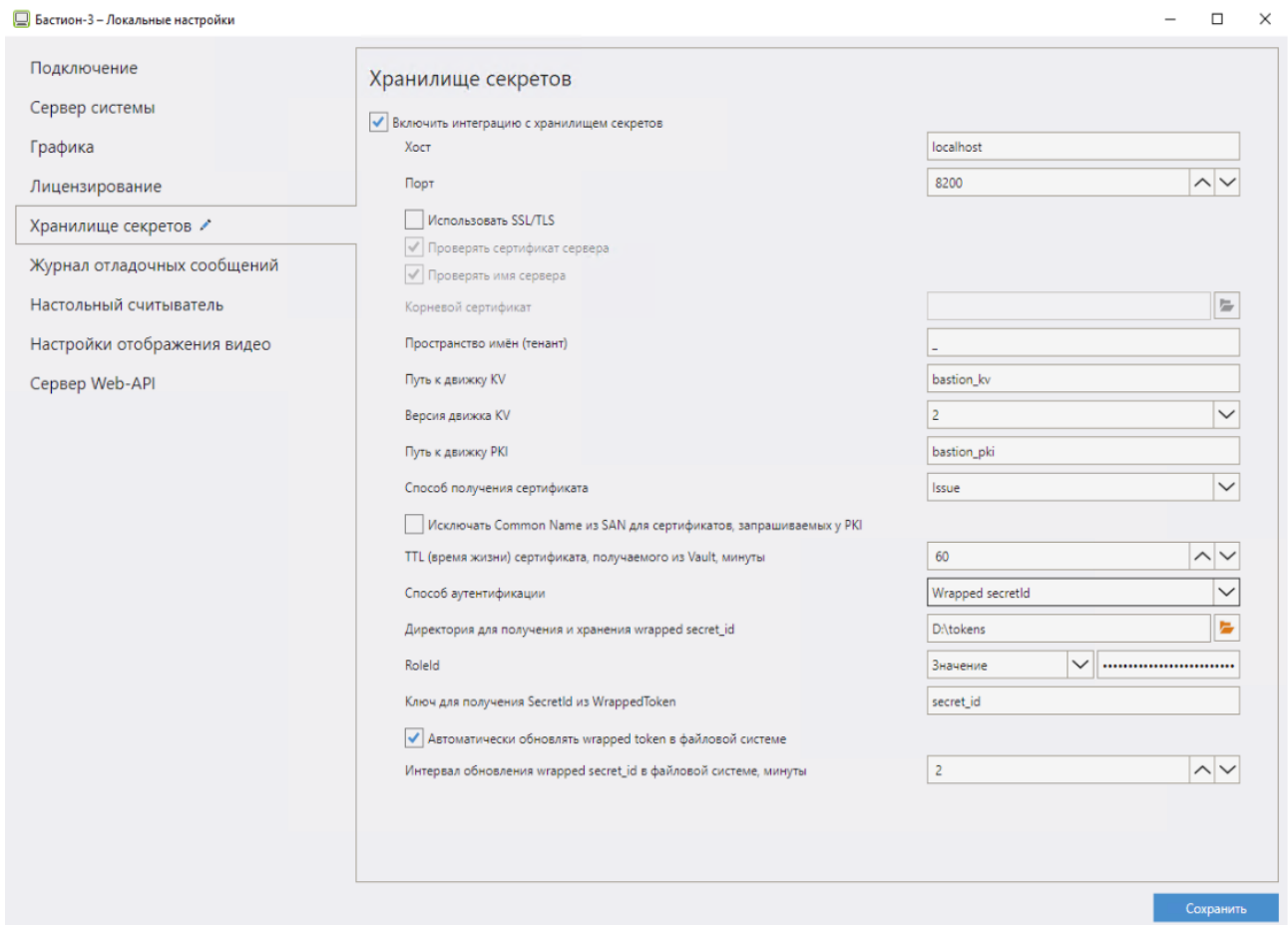


Рис. 1. Настройка подключения к хранилищу секретов

Далее, необходимо настроить, в соответствии с настройками хранилища секретов, следующие параметры (их значения следует уточнить у администратора хранилища секретов):

Хост – сервер, где расположено хранилище секретов.

Порт – порт, который будет использоваться для подключения к хранилищу секретов.

Использовать SSL/TLS – использовать ли защищенное подключение к хранилищу секретов.

Проверять сертификат сервера – если включено, клиент будет проверять действительность сертификата сервера хранилища секретов при подключении.

Проверять имя сервера – если включено, при проверке сертификата сервера хранилища сертификатов будет проверяться, что сертификат выдан серверу с именем, совпадающим с параметром Хост.

Корневой сертификат – сертификат, который должен быть в цепочке доверия сертификата сервера хранилища секретов.

Пространство имён (тенант) – пространство имен (namespace) для обеспечения изоляции на уровне тенанта. Если используемый экземпляр Vault не сконфигурирован на использование пространств имён, значение этого параметра будет игнорироваться.

Путь к движку KV – путь, по которому будут производиться обращения к движку Key/Value в хранилище секретов для получения статичных секретов по ключу.

Способ получения сертификата – способ получения сертификата из Vault. Доступны варианты:



- Issue – стандартный способ запроса получения сертификата из Vault, когда и сертификат и приватный ключ генерируются и возвращаются Vault;
- Sign – способ, требующий генерацию приватного ключа на стороне клиентской системы. При этом для запроса сертификата используется Certificate Signing Request. Набор настраиваемых для получения сертификата параметров расширяется дополнительным параметром – DistinguishedName (уникальное имя для сертификата).
- Fetch – способ, применимый для SecMan. От Sign отличается наличием дополнительного параметра – Email, а также тем, что если сертификат с запрашиваемыми параметрами уже существует, то будет возвращён он вместо генерации нового сертификата.

Версия движка KV – 1 или 2, в зависимости от используемой версии в хранилище секретов.

Путь к движку PKI – путь, по которому будут производиться обращения к движку Public Key Infrastructure в хранилище секретов (используется для получения сертификатов).

Исключать Common Name из SAN для сертификатов, запрашиваемых у PKI – параметр, который используется для управления тем, включать ли Common Name (CN) в список Subject Alternative Names (SANs) при запросе сертификата.

TTL (время жизни) сертификата, получаемого из Vault, минуты – определяет, в течении какого периода времени сертификаты, получаемые из Vault, будут действительны.

В системе доступно 3 вида аутентификации в хранилище:

1. *Token*. Базовый метод аутентификации. Аутентификационный токен можно получать в виде непосредственного значения, из переменной среды, или из CLI (командой).
2. *AppRole*. Аутентификация производится по RoleId (идентификатор роли в Vault) и SecretId (секретная часть). И RoleId, и SecretId можно получать одним из трёх способов: в виде непосредственного значения, из переменной среды, или из CLI (командой).
3. *Wrapped SecretId*. Аналогичен методу AppRole, но в отличие от предыдущего способа, SecretId доставляется в виде так называемого wrapped token, который предназначен для одноразового запроса SecretId из хранилища секретов.

Для этого способа аутентификации дополнительно требуется указать:

*Директория для получения и хранения wrapped secret_id – каталог, который будет использоваться в файловой системе для получения и хранения файла с wrapped token, содержащим SecretId. На момент запуска сервисов ПК «Бастион-3»: Локального агента или сервера Web-API в указанном каталоге должен содержаться файл LocalAgent.token или VwebAPI.token соответственно. Файл должен содержать корректный и непросроченный wrapped token с актуальным и пригодным для аутентификации SecretId. Если не включена опция *Автоматически обновлять wrapped token в файловой системе*, то при перезапуске сервисов ПК «Бастион-3» наличие в каталоге файлов с пригодными wrapped token должно поддерживаться внешними средствами.*

RoleId – идентификатор роли для AppRole.

Ключ для получения SecretId из WrappedToken – ключ, по которому можно получить значение SecretId из wrapped token (wrapped).

Автоматически обновлять wrapped token в файловой системе – система будет перечитывать файл завернутого токена один раз в указанный интервал времени.

Способ аутентификации следует согласовать с администратором хранилища секретов.



2.2.2. Настройка с помощью консольной утилиты BCnfg

Использование:

```
bcnfg vault [команда []]
```

Доступные команды:

```
view    просмотр параметров интеграции с хранилищем секретов
set     задание параметров интеграции с хранилищем секретов
```

Доступные параметры:

```
--format=<text|xml|json>
    формат вывода настроек при выполнении команды view
    (по умолчанию: text)
--use_secrets_storage=<on|off>
    включить/выключить получение секретов из хранилища секретов
    (по умолчанию: off)
--host=ИМЯ
    имя/адрес сервера хранилища секретов
    (по умолчанию: localhost)
--port=ПОРТ
    номер порта сервера хранилища секретов
    (по умолчанию: 8200)
--use_ssl=<on|off>
    включить/выключить использование SSL/TLS
    при подключении к хранилищу секретов
    (по умолчанию: off)
--validate_server_certificate=<on|off>
    проверять сертификат сервера хранилища секретов
    (по умолчанию: off)
--validate_server_certificate_common_name=<on|off>
    проверять имя сервера хранилища секретов
    (по умолчанию: off)
--root_cert_file=ПУТЬ
    путь к файлу корневого сертификата
--namespace=NAMESPACE
    пространство имён ( )
--kv_engine_path=ПУТЬ
    путь к движку KV (по умолчанию: secret)
--kv_engine_version=<1|2>
    версия движка KV
    (по умолчанию: 1)
--pki_engine_path=
    путь к движку PKI
    (по умолчанию: pki)
--certificate_retrieval_method=<issue|sign|fetch>
    способ получения сертификатов
--auth_method=<wrapped_secret_id|token|app_role>
    способ аутентификации в хранилище секретов
--wrapped_token_dir=
    директория для получения и хранения wrapped_secret_id
    Значение используется только при способе аутентификации Wrapped secretId
    (--auth_method=wrapped_secret_id)
--secret_id_key=КЛЮЧ
    ключ для получения SecretId из WrappedToken
    (по умолчанию: secret_id)
    Значение используется только при способе аутентификации Wrapped secretId
    (--auth_method=wrapped_secret_id)
```



```
--refresh_wrapped_token=<on|off>
    автоматически обновлять wrapped token в файловой системе
    (по умолчанию: off)
    Значение используется только при способе аутентификации Wrapped secretId
    (--auth_method=wrapped_secret_id)
--refresh_wrapped_token_interval=
    интервал обновления wrapped secret_id в файловой системе в минутах (по умолчанию:
5)
    Значение используется только при способе аутентификации Wrapped secretId
    (--auth_method=wrapped_secret_id)
--role_id=SECRET_SOURCE
    параметры источника RoleId
    Значение используется только при способах аутентификации Wrapped secretId
    (--auth_method=wrapped_secret_id) и AppRole (--auth_method=app_role)
    Формат SECRET_SOURCE: тип_источника[:параметр источника].
    :
    notSet - источник не задан. Используется для сброса RoleId.
    direct:ЗНАЧЕНИЕ_ROLE_ID - в качестве источника RoleId используется явно
заданное значение.
    env:ИМЯ_ПЕРЕМЕННОЙ - в качестве источника RoleId используется значение заданной
переменной окружения.
    shell:КОМАНДА - в качестве источника RoleId используется результат выполнения
внешней команды.
    должна вывести RoleId на устройство стандартного вывода и завершиться с кодом 0.

--secret_id=SECRET_SOURCE
    параметры источника SecretId
    Значение используется только при способе аутентификации AppRole
    (--auth_method=app_role)
    Формат SECRET_SOURCE: тип_источника[:параметр источника]. Доступные источники:
    notSet - источник не задан. Используется для сброса SecretId.
    direct:ЗНАЧЕНИЕ_SECRET_ID - в качестве источника SecretId используется явно
заданное значение.
    env:ИМЯ_ПЕРЕМЕННОЙ - в качестве источника SecretId используется значение заданной
переменной окружения.
    shell:КОМАНДА - в качестве источника SecretId используется результат выполнения
внешней команды. Команда должна вывести SecretId на устройство стандартного вывода и
завершиться с кодом 0.
--token=SECRET_SOURCE
    параметры источника токена аутентификации
    Значение используется только при способе аутентификации по токenu
    (--auth_method=token)
    Формат SECRET_SOURCE: тип_источника[:параметр источника]. Доступные источники:
    notSet - источник не задан. Используется для сброса токена аутентификации.
    direct:ЗНАЧЕНИЕ_SECRET_ID - в качестве источника токена аутентификации используется
явно заданное значение.
    env:ИМЯ_ПЕРЕМЕННОЙ - в качестве источника токена аутентификации используется
значение заданной переменной окружения.
    shell:КОМАНДА - в качестве источника токена аутентификации используется результат
выполнения внешней команды. Команда должна вывести токен на устройство стандартного вывода и
завершиться с кодом 0.
--exclude_common_name=<on|off>
    исключать Common Name из SAN для сертификатов, запрашиваемых у PKI
    (по умолчанию: off)
```

--cert_ttl=МИНУТЫ
 время жизни (TTL) сертификата, запрашиваемого у хранилища секретов, в минутах

2.3. Настройка путей к секретам в хранилище

Для каждого секрета, который должен присутствовать в хранилище секретов, необходимо настроить способ его получения «Хранилище секретов» и путь к секрету в хранилище.

Пути состоят из двух частей: это путь к секрету и ключ к значению в секрете (каждый секрет сам из себя представляет словарь, набор элементов типа ключ-значение). Поэтому пути к секретам должны быть в виде "bastion3!/secret_word1", где "!" - это разделитель.

Например, на [Рис. 2](#) представлена настройка получения секретного слова для аутентификации служб из хранилища секретов.

Полный список секретов, хранение которых можно перенести в хранилище, приведён в [Приложении](#).

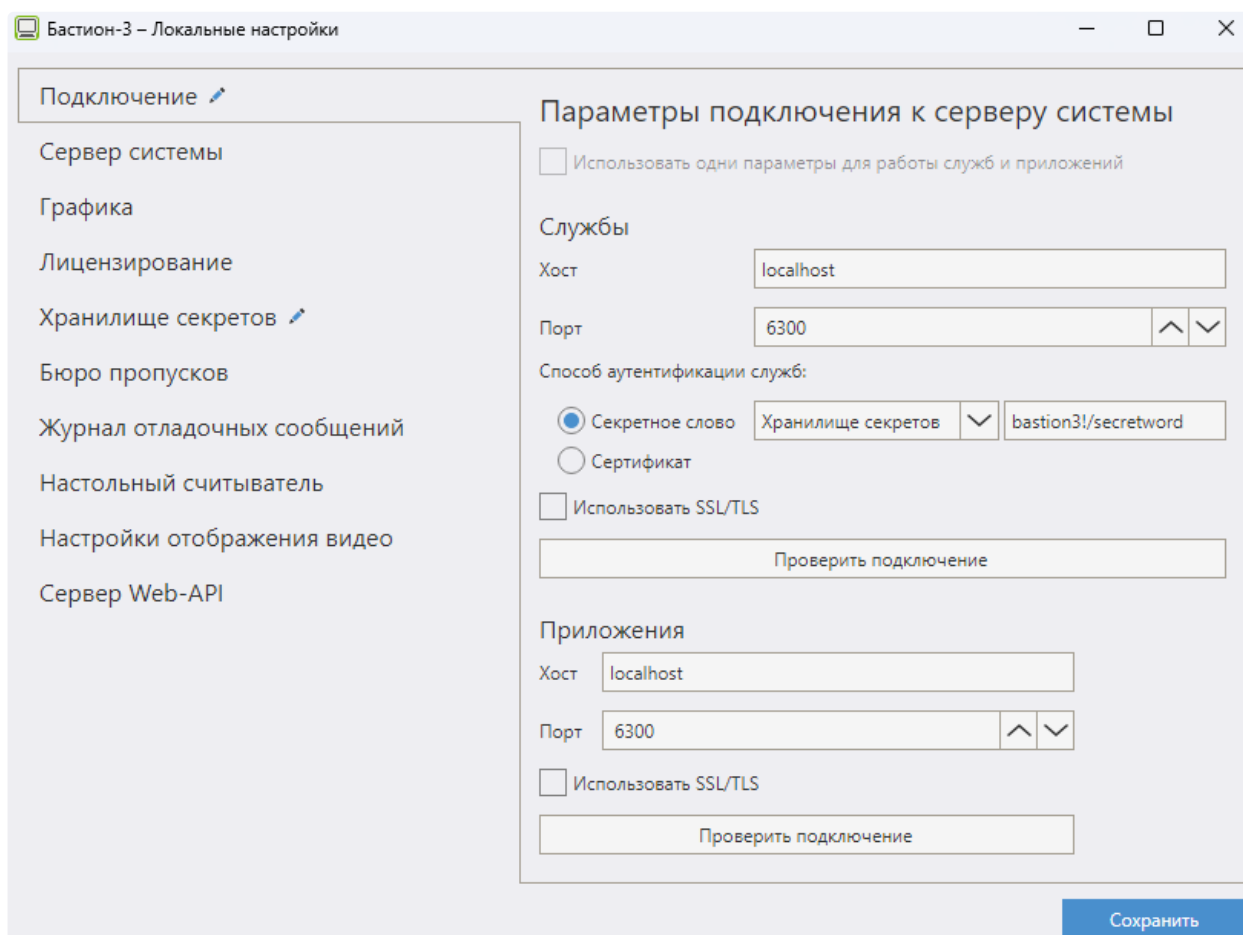


Рис. 2. Настройка получения секрета из хранилища

В случае, когда из хранилища секретов необходимо получить сертификат, следует указать параметры этого сертификата. Хранилище секретов может генерировать новый сертификат при каждом подключении с указанными параметрами. В качестве параметров можно указывать роль, common name, а также набор дополнительных идентификаторов (Subject Alternative Names, SAN).

Например, на [Рис. 3](#) приведена настройка получения клиентского сертификата из хранилища секретов со следующими параметрами: Роль: b3client, Common Name: bastion3, DNS Subject Alternative Name: smr0025.

Для получение корневого сертификата указывать параметры не требуется. Для всех сертификатов будет использоваться один корневой сертификат.

Отправлять сертификат клиента

Сертификат клиента

Роль

CN

DNS SAN

IP SAN

URI SAN

Other SAN

Email

Рис. 3. Настройка получение сертификата из хранилища

3. Приложения

3.1. Приложение 1. Список секретов

Секрет	Место настройки	Необходимые параметры
Способ аутентификации служб / секретное слово	Локальные настройки / Подключение	Путь
Сертификат клиента	Локальные настройки / Подключение (службы)	Параметры сертификата
Корневой сертификат	Локальные настройки / Подключение (службы)	Нет
Секретное слово	Локальные настройки / Сервер системы	Путь
Сертификат сервера системы	Локальные настройки / Сервер системы	Параметры сертификата
Корневой сертификат сервера системы	Локальные настройки / Сервер системы	Нет
База данных, пароль для подключения	Локальные настройки / Сервер системы	Путь
База данных, клиентский сертификат	Локальные настройки / Сервер системы	Параметры сертификата
База данных, корневой сертификат	Локальные настройки / Сервер системы	Нет
Сервер Web-API, Сертификат клиента	Локальные настройки / Сервер Web-API	Параметры сертификата
Сервер Web-API, Корневой сертификат	Локальные настройки / Сервер Web-API	Нет
Сервер Web-API, Сертификат сервера	Локальные настройки / Сервер Web-API	Параметры сертификата
Сервер Web-API, Корневой сертификат	Локальные настройки / Сервер Web-API	Нет



Пароль для сервера исходящей почты	Панель управления / Структура объекта / Настройки почты	Путь
Пароль SMPP для «Бастيون-3 – Информ»	Панель управления / Информ	Путь
Telegram Token для «Бастيون-3 – Информ»	Панель управления / Информ	Путь
Сертификат для подключения к OpenID Connect	Панель управления / Операторы и полномочия / Политики безопасности / Авторизация через OpenID Connect	Параметры сертификата
Корневой сертификат для подключения к OpenID Connect	Панель управления / Операторы и полномочия / Политики безопасности / Авторизация через OpenID Connect	Нет
Пароль для авторизации на сервере LDAP	Панель управления / Операторы и полномочия / Политики безопасности / Авторизация LDAP	Путь
Секретное слово для подключений ПЦН	Панель управления / ПЦН / Центр	Путь
Сертификат для подключений ПЦН	Панель управления / ПЦН / Центр	Параметры сертификата
Корневой сертификат для подключений ПЦН	Панель управления / ПЦН / Центр	Нет
Секретное слово для подключений репликации	Панель управления / Репликация / Филиалы репликации	Путь
Сертификат для подключений репликации	Панель управления / ПЦН / Филиалы репликации	Параметры сертификата
Корневой сертификат для подключений репликации	Панель управления / ПЦН / Филиалы репликации	Нет
SNMP Agent, V1GetCommunity	Панель управления / SNMP Агент / Настройки	Путь
SNMP Agent, V1SetCommunity	Панель управления / SNMP Агент / Настройки	Путь
SNMP Agent, V2GetCommunity	Панель управления / SNMP Агент / Настройки	Путь
SNMP Agent, V2SetCommunity	Панель управления / SNMP Агент / Настройки	Путь



SNMP Agent, V3Password	Панель управления / SNMP Агент / Настройки	Путь
SNMP Agent, V3PrivacyPhrase	Панель управления / SNMP Агент / Настройки	Путь
СС ТМК, Пароль	Панель управления / СС ТМК	Путь
СС ТМК, Сертификат	Панель управления / СС ТМК	Параметры сертификата
СС ТМК, Корневой сертификат	Панель управления / СС ТМК	Нет
ОПС Сервер, Сертификат	Панель управления / ОПС Сервер / Настройки	Параметры сертификата
ОПС Сервер, Корневой сертификат	Панель управления / ОПС Сервер / Настройки	Нет
Все пароли драйверов (поля типа Pass), помеченные атрибутом "IsSecretSourceSupported"	Универсальный конфигуратор драйверов	Путь