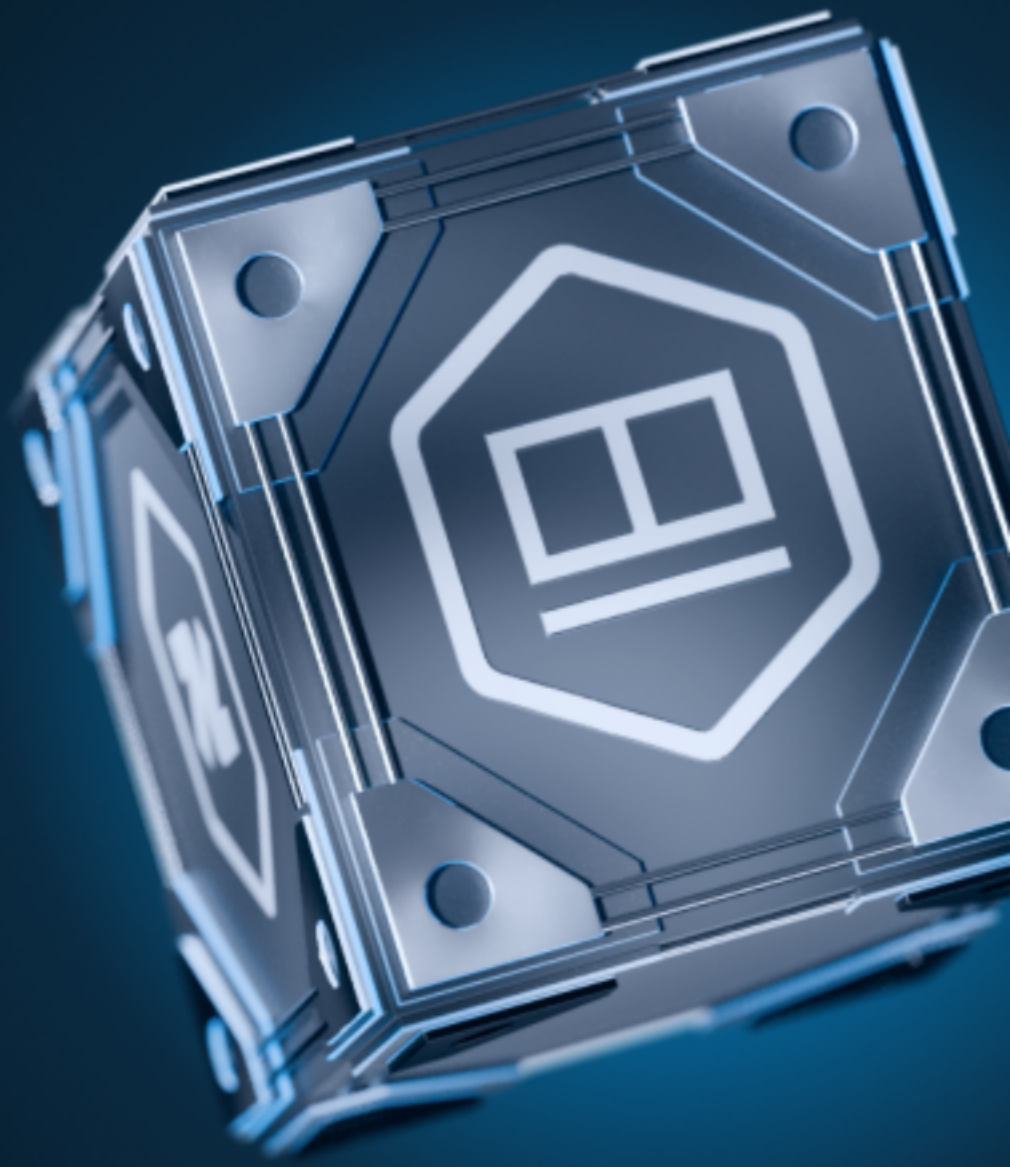
TERMIDESK VDI



Руководство администратора

Настройка компонента «Агент»

СЛЕТ.10001-01 90 04

Версия 7.0.2. Выпуск от 15.09.2026

Оглавление

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ . . . 3
АГЕНТ. ОБЩИЕ СВЕДЕНИЯ . . . 4
АГЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ . . . 6
АГЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ . . . 13
ОС Astra Linux Special Edition . . . 13
ОС Альт Рабочая станция . . . 21
Другие ОС Linux . . . 27
ОС Microsoft Windows . . . 29
АГЕНТ. НАСТРОЙКИ . . . 38
Переменные окружения и аргументы командной строки . . . 38
Агент BPM . . . 46
Конфигурационные файлы Агента BPM . . . 46
Настройка для ОС Astra Linux Special Edition . . . 56
Настройка для ОС Microsoft Windows . . . 67
Хранение информации о сессии пользователя . . . 78
Агент виртуальных смарт-карт . . . 80
Настройка Агента виртуальных смарт-карт . . . 80
Видеоагент . . . 81
Настройка видеоагента . . . 81
Агент узла виртуализации . . . 81
Использование альтернативного механизма сброса сессий . . . 82
Сессионный Агент . . . 84
Конфигурационные файлы сессионного Агента . . . 84
Первичная настройка . . . 94
Настройка сессионного Агента на использование протокола HTTPS . . . 94
Активация роли терминального сервера в ОС Microsoft Windows Server . . . 95
АГЕНТ. ЖУРНАЛИРОВАНИЕ . . . 96
АГЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ . . . 101
ТЕРМИНЫ . . . 102
СОКРАЩЕНИЯ . . . 104

ОБЩИЕ СВЕДЕНИЯ О ДОКУМЕНТЕ

Назначение документа

Настоящий документ является четвертой частью руководства администратора на программный комплекс «Диспетчер подключений виртуальных рабочих мест Термидеск» (далее - Termidesk VDI, Termidesk VDI). Документ предназначен для администраторов системы и сети.

В этом руководстве приведено назначение, установка и настройка компонента «Агент». Для того, чтобы получить информацию о месте компонента в программном комплексе, необходимо обратиться ко второй части руководства администратора - СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Типографские соглашения

Приняты следующие типографские соглашения:

- моноширинный шрифт – используется для выделения фрагментов текста программ, наименований файлов и папок (директорий), наименований пакетов, путей перемещения, строк комментариев, различных программных элементов (объект, класс, тип, переменная, команда, макрос и т. д.), а также вводимого и выводимого текста в режиме командной строки;
- «кавычки» – текст, заключенный в кавычки, используется для обозначения наименований документов, названий компонентов Termidesk VDI, пунктов меню, наименований окон, вкладок, полей, других элементов графического интерфейса, а также вводимого и выводимого текста в режиме графического интерфейса;
- **[квадратные скобки]** – текст, заключенный в квадратные скобки, используется для наименования экранных кнопок;
- **<угловые скобки>** – текст, заключенный в угловые скобки, используется для наименования клавиш клавиатуры.

АГЕНТ. ОБЩИЕ СВЕДЕНИЯ

Назначение компонента «Агент»

Компонент «Агент» (далее - Агент) входит в состав Termidesk VDI.

К компоненту Агент относятся следующие подкомпоненты, каждый из которых устанавливается отдельно:

- «Агент виртуального рабочего места» (далее - Агент ВРМ) - устанавливается в гостевую операционную систему (ОС) при подготовке базового виртуального рабочего места (ВРМ) или на терминальный сервер. Выполняет взаимодействие с компонентом «Универсальный диспетчер», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений;
- «Агент узла виртуализации» (далее - Агент УВ) - устанавливается на узел виртуализации (УВ). Агент УВ взаимодействует с гипервизором через модуль `libvirt`;
- «Сессионный агент» (далее - сессионный Агент) - устанавливается на терминальный сервер, активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям;
- «Видеоагент» (далее - видеоагент) - устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ;
- «Агент виртуальных смарт-карт» (далее - Агент виртуальных смарт-карт, Агент смарт-карт) - устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ.

Соответствие перечисленных подкомпонентов установочным файлам приведено в таблице (см. таблицу Соответствие подкомпонентов и наименований установочных файлов).

Таблица 1. Соответствие подкомпонентов и наименований установочных файлов

Наименование подкомпонента	Место установки подкомпонента	Наименование пакета установки
Агент ВРМ	Гостевая ОС, ОС терминального сервера или ОС автономной машины	`termidesk-agent`
Агент УВ	ОС с ПК СВ Брест	`termidesk-vmsd`
Сессионный Агент	ОС терминального сервера	`termidesk-session-agent`
Видеоагент	Гостевая ОС	`termidesk-video-agent`
Агент смарт-карт	Гостевая ОС	`termidesk-pcsc-vscard`

Агент УВ (сервис `termidesk-vmsd`) запускается на узлах программного комплекса «Средства виртуализации «Брест» (далее - ПК СВ Брест) и работает в качестве посредника между `libvirtd` и Агентом ВРМ через `virtio` канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

Полученные от Агента ВРМ команды (`shutdown`, `disconnect`), `termidesk-vmsd` транслирует в `libvirtd`, позволяя тем самым управлять ВМ, на которой запущен Агент ВРМ.

Видеоагент (сервис `termidesk-video-agent`) запускается в ВРМ и предназначен для приема изображения с камеры пользовательской рабочей станции через `virtio` канал `/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`. Полученный поток перенаправляется на предварительно созданную виртуальную видеокамеру, что позволяет приложениям видеоконференций работать внутри ВРМ.

Требования к аппаратному и программному обеспечению

Для установки подкомпонентов Агента минимальные аппаратные требования узла должны соответствовать следующим:

- процессор архитектуры Intel x86 разрядности 64 бит. Для некоторых ОС поддерживаются другие архитектуры, это указано в списке поддерживаемых ОС;
- оперативная память, не менее 1 ГБ;
- свободное дисковое пространство, не менее 200 МБ;
- сетевое соединение, не менее 100 Мбит/с.

Требования к программному обеспечению для подкомпонентов приведены в таблице (см. таблицу Перечень требований к программному обеспечению).

Таблица 2. Перечень требований к программному обеспечению

Агент ВРМ	Видеоагент и Агент смарт-карт	Агент УВ	Сессионный Агент
ОС: • Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • Альт Рабочая станция 10; • Альт Рабочая станция 11; • Microsoft Windows 10 1809 LTS • Microsoft Windows 11 LTSC 2024; • Microsoft Windows Server 2022	ОС: • Astra Linux Special Edition 1.7 (1.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • Альт Рабочая станция 10; • Альт Рабочая станция 11; • Microsoft Windows 10 1809 LTS • Microsoft Windows 11 LTSC 2024; • Microsoft Windows Server 2022	ОС: • Astra Linux Special Edition 1.7 (.7.5, 1.7.6, 1.7.7, 1.7.8, 1.7.9); • Astra Linux Special Edition 1.8 (1.8.3, 1.8.4, 1.8.5, 1.8.6); • РЕД ОС 7.3; • РЕД ОС 8; • CentOS 8	ОС: • Astra Linux Special Edition Server 1.8 (1.8.1, 1.8.2, 1.8.4, 1.8.5, 1.8.6); • Альт Рабочая станция 10; • Microsoft Windows Server 2016; • Microsoft Windows Server 2019; • Microsoft Windows Server 2022 В ОС должны быть установлены: • компонент «Сервер терминалов Astra Linux» для ОС Astra Linux Special Edition (Server); • MS RDS для ОС Microsoft Windows Server

Указанный в таблице компонент «Сервер терминалов Astra Linux» является компонентом Termidesk VDI.

В платформе виртуализации для видеоагента должен быть активирован канал `/dev/virtio-ports/ru.termidesk.RealtimeStreaming.0`.

В платформе виртуализации для Агента УВ должен быть активирован канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

АГЕНТ. ПОЛУЧЕНИЕ ПАКЕТОВ УСТАНОВКИ

Получение пакетов установки через Интернет-репозиторий

Для получения пакетов установки может использоваться Интернет-репозиторий: https://repos.termidesk.ru/.

Для подключения репозитория в ОС Astra Linux Special Edition нужно:

- установить пакеты:

```
sudo apt install -y lsb-release wget apt-transport-https debian-keyring
```

где:

`-y` - ключ для пропуска подтверждения установки;

- добавить Интернет-репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `https://repos.termidesk.ru/astra`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.8_x86-64 non-free" > /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

    `deb https://repos.termidesk.ru/astra <…>` - добавляемый репозиторий;

    Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

      ```
      sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat /etc/astra_version) non-free" >
      ```

```
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

- добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

- для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
  - подключить три репозитория:

```
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(cat
/etc/astra_version) non-free" >>
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb https://repos.termidesk.ru/astra $(lsb_release -cs
2> /dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

  - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- получить ключ репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его в ОС:
  - для ОС Astra Linux Special Edition 1.7:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-
PUBLIC | sudo apt-key add -
```

- для ОС Astra Linux Special Edition 1.8:

```
wget --no-check-certificate -qO - https://repos.termidesk.ru/astra/GPG-KEY-PUBLIC |  sudo gpg --dearmour -o /etc/apt/trusted.gpg.d/termidesk.gpg
```

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.



Команды добавления ключа репозитория Termidesk VDI отличаются в зависимости от используемой версии ОС.

Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

Получение пакетов установки в ОС Astra Linux Special Edition

Дистрибутив представлен бинарным файлом пакета ПО в `deb`-формате. Установка в ОС Astra Linux Special Edition производится из локального репозитория, распространяемого в формате `iso`-образа.

Получить `iso`-образ можно двумя способами:

- заполнив запрос через сайт Termidesk VDI: https://termidesk.ru/support/#request-support;
- через личный кабинет:https://lk.astra.ru/.

Для подключения локального репозитория Termidesk VDI на узле, где предполагается установка, нужно:

- скопировать в домашний каталог пользователя образ диска `termidesk-<версия>.iso`;
- подключить образ диска к файловой системе в каталог `/mnt`:

```
sudo mount -o loop termidesk-<версия>.iso /mnt
```

где:

`-o loop` - параметры для привязки петлевого устройства (`/dev/loop`) к файлу `termidesk-<версия>.iso`, устройство затем монтируется в указанный каталог `/mnt`;

- скопировать содержимое каталога `repos` подключенного образа диска в каталог `/var` локальной файловой системы:

```
sudo cp -Rp /mnt/repos /var
```

где:

`-Rp` - ключ для рекурсивного копирования подкаталогов и файлов с сохранением исходных свойств;

- отключить подключенный ранее образ диска от узла:

```
sudo umount /mnt
```

- установить пакет `lsb-release`:

```
sudo apt install -y lsb-release
```

- добавить локальный репозиторий Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list` через командный интерпретатор `sh`:
  - выяснить установленную версию ОС:

    ```
    sudo cat /etc/astra_version
    ```

  - определить актуальное имя каталога с пакетами в `/var/repos`;
  - указать в файле конфигурации APT корректное (фактическое) имя каталога:

    ```
    sudo sh -c 'echo "deb file:/var/repos/astra 1.8_x86-64 non-free" >
    /etc/apt/sources.list.d/termidesk_local.list'
    ```

    где:

    `-c` - ключ для чтения команд из вводимой строки (стандартный ввод);

    `echo` - команда вывода текста, совместно с символом «>» используется для перенаправления строки в файл;

`deb file:/var/repos/astra 1.8_x86-64 non-free` - добавляемый репозиторий с вложенной командой получения версии ОС;



Приведенный пример команды актуален для установки основных компонентов Termidesk, пакеты которых расположены в каталоге `1.8_x86-64`.

- для корректной установки компонентов TERA потребуется корректно подключить дополнительные репозитории и настроить их приоритет:
  - для версий ОС Astra Linux Special Edition меньше или равных 1.7.6, а также для версий 1.8.X:
    - подключить два репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" > /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - добавить повышенный приоритет для репозитория с требуемой версией ОС (значение `$(cat /etc/astra_version)` может подходить не для всех репозиториев, т.к. версия может указываться без точек - в этом случае нужно вручную указать корректную версию):

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000
EOF"
```

  - для версий ОС Astra Linux Special Edition 1.7.7 и 1.7.8:
    - подключить три репозитория:

```
sudo sh -c 'echo "deb file:/var/repos/astra 1.7.6 non-free" >
/etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(cat /etc/astra_version)
non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
sudo sh -c 'echo "deb file:/var/repos/astra $(lsb_release -cs 2>
/dev/null) non-free" >> /etc/apt/sources.list.d/termidesk_local.list'
```

    - настроить два приоритета:

```
sudo bash -c "cat << 'EOF' > /etc/apt/preferences.d/uveon-priority
Package: *
Pin: release n=1.7.6
Pin-Priority: 950

Package: *
```

```
Pin: release n=$(cat /etc/astra_version)
Pin-Priority: 1000

EOF"
```

- выполнить поиск ключа репозитория Termidesk VDI `GPG-KEY-PUBLIC` и добавить его:

```
sudo cat /var/repos/astra/GPG-KEY-PUBLIC | sudo gpg --dearmour -o
/etc/apt/trusted.gpg.d/termidesk.gpg
```

- убедиться, что ключ `release@uveon.ru` был успешно добавлен:

```
apt-key list
```



В случае, если ключ не отображен в выводе команды, необходимо убедиться, что ключ `GPG-KEY-PUBLIC` существует:

```
cat /var/repos/astra/GPG-KEY-PUBLIC
```

Если ключ все же существует, следует проверить правильность выполнения шагов по добавлению репозитория Termidesk VDI в файл `/etc/apt/sources.list.d/termidesk_local.list`.

При успешном выполнении всех шагов команда выведет содержимое ключа в формате Base64.

В зависимости от используемой версии ОС команды добавления ключа репозитория Termidesk VDI могут отличаться. Если для ОС Astra Linux Special Edition 1.8 ключ репозитория был добавлен командой, применимой к другой версии ОС, то для исправления нужно:

- узнать идентификатор добавленного ключа репозитория:

```
apt-key list
```

- удалить ключ:

```
apt-key --keyring /etc/apt/trusted.gpg del 4E1632CC
```

где `4E1632CC` - последние 8 символов идентификатора ключа;

- вновь добавить ключ репозитория.

- обновить данные пакетного менеджера:

```
sudo apt update
```

- проверить настройку приоритетов репозиториев:

```
apt-cache policy
```

Команду `sudo apt update` необходимо выполнять при каждом изменении списка источников пакетов или при изменении содержимого этих источников.

АГЕНТ. УСТАНОВКА, ОБНОВЛЕНИЕ И УДАЛЕНИЕ

ОС Astra Linux Special Edition

Установка Агента BPM в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Для установки Агента BPM в гостевой ОС:

- выполнить:

```
sudo apt install termidesk-agent
```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента BPM. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.



Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента BPM**);
- через вызов программы `termidesk-agent-config`:

```
sudo termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
termidesk-agent
```

где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `agent.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;
- `TDSK_LOG_SRV_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- `TDSK_LOG_USER_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

В состав пакета `termidesk-agent` входят:

- `termidesk-agent-config` - программа, осуществляющая настройку Агента ВРМ;
- `termidesk-agent-user` - программа, отслеживающая состояние пользовательской сессии и отображающая иконку Агента ВРМ в системном трее;
- `termidesk-agent-daemon` - служба, регистрирующая ВМ в компоненте «Универсальный диспетчер», принимающая и обрабатывающая команды;
- `termidesk-cupsd` - служба, динамически обновляющая список принтеров.



После установки Агент ВРМ обязательно должен быть настроен согласно подразделу **Настройка для ОС Astra Linux Special Edition**.

Проверка состояния службы Агента ВРМ выполняется командой:

```
sudo systemctl status termidesk-agent
```

Проверка состояния службы `termidesk-cupsd` выполняется командой:

```
sudo systemctl status termidesk-cupsd
```

Установка видеоагента в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Перед установкой видеоагента (служба `termidesk-video-agent`) необходимо:

- установить пакет `linux-headers`, соответствующий ядру, загруженному в работающей ОС:

```
sudo apt install linux-headers-`uname -r`
```



Если видеоагент устанавливается не в ОС Astra Linux Special Edition следует

> учесть, что наименование пакета заголовочных файлов ядра может отличаться от `linux-headers`.

- если видеоагент должен быть установлен в ОС с включенным режимом замкнутой программной среды (ЗПС) нужно:
  - удостовериться, что используемая версия ОС - 1.7.5 и выше;
  - затем установить пакет `v4l2loopback-kmod`, соответствующий ядру, загруженному в работающей ОС:

```
sudo apt install v4l2loopback-kmod-`uname -r`
```

Установка видеоагента выполняется в гостевой ОС командой:

```
sudo apt install termidesk-video-agent
```

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-video-agent`:

```
sudo systemctl enable termidesk-video-agent.service
sudo systemctl start termidesk-video-agent.service
```

Проверить состояние службы:

```
sudo systemctl status termidesk-video-agent.service
```

Установка Агента смарт-карт в ОС Astra Linux Special Edition

Перед установкой необходимо подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**.

Установка Агента смарт-карт выполняется в гостевой ОС командой:

```
sudo apt install termidesk-pcsc-vscard
```

После установки Агент смарт-карт должен быть настроен согласно подразделу **Настройка Агента виртуальных смарт-карт**.

Установка Агента УВ в ОС Astra Linux Special Edition

Агент УВ (сервис `termidesk-vmsd`) запускается на узлах виртуализации ПК СВ Брест и работает в качестве посредника между `libvirtd` и Агентом ВРМ через `virtio`-канал `/dev/virtio-ports/ru.termidesk.tvm.0`.

Полученные от Агента ВРМ команды (`shutdown`, `disconnect`), `termidesk-vmsd` транслирует в `libvirtd`, позволяя тем самым управлять ВМ, на которой запущен Агент ВРМ.

Агент УВ устанавливается из `deb`-пакета `termidesk-vmsd`.

Перед установкой необходимо обязательно удалить предыдущую версию!

Для установки Агента УВ нужно:

- подключить репозиторий Termidesk VDI, как указано в подразделе как указано в подразделе **Получение пакетов установки**;
- выполнить:

```
sudo apt install termidesk-vmsd
```

- убедиться, что пользователь, от имени которого запущена служба `termidesk-vmsd`, добавлен в группы `libvirt`, `libvirt-admin`, `libvirt-qemu` и `kvm`.

После установки рекомендуется выполнить перезагрузку узла виртуализации.

Установка сессионного Агента в ОС Astra Linux Special Edition

Сессионный Агент устанавливается на терминальном сервере ОС Astra Linux Special Edition (Server) из `deb`-пакета `termidesk-session-agent`.

Для установки сессионного Агента:

- подключить репозиторий Termidesk VDI, как указано в подразделе **Получение пакетов установки**;
- выполнить:

```
sudo apt install termidesk-session-agent
```

- в окне «Лицензионное соглашение» ознакомиться с соглашением и нажать экранную кнопку **[Выход]**;
- на запрос «Принимаете ли вы условия лицензионного соглашения?» подтвердить принятие соглашения, нажав экранную кнопку **[Принимаю]**;
- в окне «Расширенные настройки»:
  - указать путь к каталогу хранения файлов конфигурации. Значение по умолчанию: `/etc/opt/termidesk-session-agent`;
  - указать путь к каталогу хранения журналов. Значение по умолчанию: `/var/log/termidesk`;
  - нажать экранную кнопку **[Далее]**;
- дождаться завершения установки.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения `DEBIAN_FRONTEND=noninteractive`, `SSA_CONFIG_DIR` и `SSA_LOG_DIR` и передать их в команду установки:

```
sudo DEBIAN_FRONTEND=noninteractive SSA_CONFIG_DIR=<путь_к_каталогу>
SSA_LOG_DIR=/<путь_к_каталогу> apt install termidesk-session-agent
```

Где:

- DEBIAN_FRONTEND=noninteractive - переменная, указывающая запуск в режиме «тихой» установки;
- SSA_CONFIG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения файлов конфигурации. Заменяет значение по умолчанию, если передается непустое значение;
- SSA_LOG_DIR=<путь_к_каталогу> - переменная, указывающая путь к каталогу хранения журналов. Заменяет значение по умолчанию, если передается непустое значение.



После установки изменить настройки можно через файл /etc/default/termidesk-session-agent.

После установки служба termidesk-session-agent автоматически запустится, также создастся конфигурационный файл session_agent.ini.



После установки сессионный Агент может быть настроен согласно подразделу **Первичная настройка**.

После установки сессионного Агента будет создан файл БД SQLite /opt/termidesk/share/termidesk-session-agent/termidesk_ssa.db, предназначенный для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Установка в режиме ЗПС

Замкнутая программная среда (ЗПС) является средством повышения безопасности ОС путем контроля целостности (неизменности) файлов.

Механизм контроля реализован в виде невыгружаемого модуля ядра ОС Astra Linux Special Edition (модуль digsig_verif), выполняющего проверку электронной цифровой подписи файлов (ЭЦП).

Перед установкой компонентов Termidesk VDI необходимо установить пакет termidesk-digsig-keys, для этого:

- подключить репозиторий Termidesk VDI или получить отдельный пакет termidesk-digsig-keys из репозитория;
- выполнить установку с использованием репозитория:

```
sudo apt -y install termidesk-digsig-keys
```

- либо выполнить установку из deb-пакета:

```
sudo apt install -y /home/user/termidesk-digsig-keys-XXXXXX_amd64.deb
```

где:

-y - ключ для пропуска подтверждения установки;

/home/user/termidesk-digsig-keys-XXXXXX_amd64.deb - расположение пакета termidesk-digsig-keys-XXXXXX_amd64.deb.

- перезагрузить ОС:

```
sudo reboot
```

- выполнить установку компонента Termidesk VDI.

Для ЗПС может быть активирован режим проверки встроенной ЭЦП в расширенных атрибутах (`DIGSIG_XATTR_MODE`). В этом случае потребуется подписать файлы, которые будут проходить проверку, имеющимися в организации ключами. Информация о процессе подписи и активации механизма проверки встроенной ЭЦП в расширенных атрибутах приведена в справочном центре Astra Linux: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Постановка Агента на контроль целостности

После установки и настройки Агентов необходимо поставить их на контроль целостности.



В подразделе приведена процедура только для Агентов, установленных в ОС Astra Linux Special Edition.

Для контроля целостности используются встроенные в ОС Astra Linux Special Edition программные средства на основе `Another File Integrity Checker`, представленного пакетом `afick`.

Настройка регламентного контроля целостности выполняется в конфигурационном файле `/etc/afick.conf`.



Настройку следует производить только после окончательного внедрения компонента, поскольку с файлов конфигурации и исполняемых файлов будут сняты эталонные контрольные суммы.

Для постановки на контроль целостности Агента ВРМ, Агента смарт-карт,видеоагента необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/termidesk PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-agent.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-cupsd.service PARSEC
/usr/bin/termidesk-agent-user PARSEC
/usr/lib/python3/dist-packages/termidesk_agent PARSEC
/usr/lib/systemd/system/termidesk-video-agent.service PARSEC
/usr/sbin/termidesk-agent-config PARSEC
/usr/sbin/termidesk-agent-daemon PARSEC
/usr/sbin/termidesk-cups-daemon PARSEC
/usr/share/doc/termidesk-agent PARSEC
/usr/share/doc/termidesk-pcsc-vscard PARSEC
/usr/share/doc/termidesk-video-agent PARSEC
/usr/share/polkit-1/actions/org.termidesk.pkexec.TermideskAgentConfig.policy PARSEC
/usr/share/termidesk-agent PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/termidesk-
cupsd.service  PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-cupsd.service.dsh-also PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-video-agent.service.dsh-also
PARSEC
```

```
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-agent.service.dsh-also PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для постановки на контроль целостности Агента УВ необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/systemd/system/multi-user.target.wants/termidesk-vmsd.service PARSEC
/usr/lib/python3/dist-packages/termidesk_agent PARSEC
/usr/lib/systemd/system/termidesk-vmsd.service PARSEC
/usr/sbin/termidesk-vmsd PARSEC
/usr/share/doc/termidesk-vmsd PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/termidesk-
vmsd.service PARSEC
/var/lib/systemd/deb-systemd-helper-enabled/termidesk-vmsd.service.dsh-also PARSEC

#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для постановки на контроль целостности сессионного Агента необходимо добавить в конфигурационный файл `/etc/afick.conf` следующие строки:

```
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/X11/Xresources/x11-stal PARSEC
/etc/X11/stal.conf PARSEC
/etc/dbus-1/system.d/ru.uveon.stal.conf PARSEC
/etc/logrotate.d/stal PARSEC
/etc/pam.d/stal PARSEC
/etc/pam.d/stal-rdp PARSEC
/etc/stal PARSEC
/etc/syslog-ng/conf.d/stal-proxy.conf PARSEC
/etc/syslog-ng/conf.d/stal-service.conf PARSEC
/etc/syslog-ng/conf.d/stal-watchdog.conf PARSEC
/etc/systemd/system/multi-user.target.wants/stal-proxy.service PARSEC
/etc/systemd/system/multi-user.target.wants/stal-watchdog.service PARSEC
/etc/systemd/system/multi-user.target.wants/termidesk-stal.service PARSEC
/etc/systemd/system/stal-proxy.service PARSEC
/etc/systemd/system/stal-watchdog.service PARSEC
/etc/systemd/system/termidesk-stal.service PARSEC
/etc/ufw/applications.d/stal-proxy PARSEC
/usr/libexec/stal PARSEC
/usr/sbin/stal_proxy PARSEC
/usr/sbin/stal_service PARSEC
/usr/sbin/stal_watchdog PARSEC
/usr/share/doc/stal PARSEC
```

```
#Репозиторий Termidesk VDI (если используется)
/var/repos/ PARSEC
```

Для снятия эталонных значений контрольных сумм используется команда:

```
afick -i
```

Для проверки соответствия контрольных сумм эталонным значениям автоматически создаются задания в системном планировщике заданий `cron`.

Для ручной проверки соответствия контрольных сумм используется команда:

```
afick -k
```



В случае отсутствия по какой-либо причине исполняемых фалов `*.pyc`, они будут повторно сгенерированы при перезапуске сервера Python. В этом случае нужно повторно проинициализировать средство регламентного контроля целостности `afick`.

Обновление Агентов в ОС Astra Linux Special Edition

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ и Агента УВ.

Для обновления Агента ВРМ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-agent
```

- установить новую версию:

```
sudo apt install -y termidesk-agent
```

Для обновления Агента УВ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-vmsd
```

- установить новую версию:

```
sudo apt install -y termidesk-vmsd
```

В случае, если обновление компонента «Универсальный диспетчер» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Astra Linux Special Edition

Удаление Агентов из среды ОС Astra Linux Special Edition выполняется командой:

```
sudo aptitude purge -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент;
- `termidesk-video-agent` - видеоагент;
- `termidesk-pcsc-vscard` - Агент смарт-карт;
- `termidesk-vmsd` - Агент УВ.

Если установка пакета производилась не из локального репозитория, удаление выполняется командой:

```
sudo dpkg -P <наименование_пакета>
```



Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

ОС Альт Рабочая станция

Установка Агента ВРМ в ОС Альт Рабочая станция

Агент ВРМ устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-agent`.

Для установки Агента ВРМ:

- (опционально) подключить Интернет-репозиторий Termidesk VDI (см. пример в подразделе **Получение пакетов установки**);
- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-agent`:
  - если установка выполняется с подключенным Интернет-репозиторием:

    ```
    apt-get install termidesk-agent
    ```

  - если установка выполняется без подключенного Интернет-репозитория:

    ```
    apt-get install <путь_к_пакету>
    ```

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента ВРМ. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.

Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента ВРМ**);
- через вызов программы `termidesk-agent-config`:

```
termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
<путь_к_пакету>
```

где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `agent.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;
- `TDSK_LOG_SRV_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- `TDSK_LOG_USER_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-agent`:

```
systemctl enable termidesk-agent.service
systemctl start termidesk-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-agent.service
```

После установки Агент ВРМ обязательно должен быть настроен.

Установка видеоагента в ОС Альт Рабочая станция

Видеоагент устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-video-agent`.

Перед установкой видеоагента необходимо:

- установить пакет `kernel-headers-modules`, соответствующий ядру, загруженному в работающей ОС, пример:

```
apt-get install kernel-headers-modules-std-def
```

Для установки видеоагента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-video-agent`:

```
apt-get install <путь_к_пакету>
```

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-video-agent`:

```
systemctl enable termidesk-video-agent.service
systemctl start termidesk-video-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-video-agent.service
```

Установка Агента смарт-карт в ОС Альт Рабочая станция

Агент смарт-карт устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-pcsc-vscard`.

Для установки сессионного Агента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-pcsc-vscard`:

```
apt-get install <путь_к_пакету>
```

После установки Агент смарт-карт должен быть настроен согласно подразделу **Настройка Агента виртуальных смарт-карт**.

Установка сессионного Агента в ОС Альт Рабочая станция

Сессионный Агент устанавливается в ОС Альт Рабочая станция из `rpm`-пакета `termidesk-session-agent`.

Для установки сессионного Агента:

- переключиться в окружение суперпользователя:

```
su -
```

- выполнить установку `termidesk-session-agent`:

```
apt-get install <путь_к_пакету>
```

- в окне «Лицензионное соглашение» ознакомиться с соглашением и нажать экранную кнопку **[Выход]**;
- на запрос «Принимаете ли вы условия лицензионного соглашения?» подтвердить принятие соглашения, нажав экранную кнопку **[Принимаю]**;
- в окне «Расширенные настройки»:
  - указать путь к каталогу хранения файлов конфигурации. Значение по умолчанию: `/etc/opt/termidesk-session-agent`;
  - указать путь к каталогу хранения журналов. Значение по умолчанию: `/var/log/termidesk`;
  - нажать экранную кнопку **[Далее]**;
- дождаться завершения установки.

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения `DEBIAN_FRONTEND=noninteractive`, `SSA_CONFIG_DIR` и `SSA_LOG_DIR` и передать их в команду установки:

```
TDSK_FRONTEND=noninteractive SSA_CONFIG_DIR=<путь_к_каталогу>
SSA_LOG_DIR=<путь_к_каталогу> apt-get install <путь_к_пакету>
```

Где:

- `TDSK_FRONTEND=noninteractive` - переменная, указывающая запуск в режиме «тихой» установки;
- `SSA_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения файлов конфигурации. Заменяет значение по умолчанию, если передается непустое значение;
- `SSA_LOG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов. Заменяет значение по умолчанию, если передается непустое значение.



После установки изменить настройки можно через файл `/etc/default/termidesk-session-agent`.

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-session-agent`:

```
systemctl enable termidesk-session-agent.service
systemctl start termidesk-session-agent.service
```

Проверить состояние службы:

```
systemctl status termidesk-session-agent.service
```



После установки сессионный Агент может быть настроен согласно подразделу **Первичная настройка**.

После установки сессионного Агента создастся конфигурационный файл `session_agent.ini`, а также файл БД SQLite `/opt/termidesk/share/termidesk-session-agent/termidesk_ssa.db`, предназначенный для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Обновление Агентов в ОС Альт Рабочая станция

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ.

Для обновления Агента ВРМ нужно:

- переключиться в окружение суперпользователя:

```
su -
```

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
apt-get remove -y termidesk-agent
```

- установить новую версию:

```
apt-get install -y termidesk-agent
```

В случае, если обновление компонента «Универсальный диспетчер» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Альт Рабочая станция

Удаление Агентов выполняется командой:

```
sudo apt-get remove -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент.



Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

Другие ОС Linux

Установка Агентов в других ОС Linux

Для установки Агентов в гостевой ОС выполнить:

```
sudo yum install <путь_к_пакету>
```

Для установки Агента ВРМ в гостевой ОС:

- выполнить:

```
sudo yum install termidesk-agent
```



В зависимости от дистрибутива ОС Linux, а именно пакетного менеджера, команда установки может отличаться от приведенной.

Для ввода гостевой ОС Debian 12/13 в домен MS AD нужно установить пакеты, которые не являются зависимостями агента: `sssd-tools`, `adcli`, `sssd`, `libnss-sss`, `libpam-sss`.

После установки Агент ВРМ обязательно должен быть настроен.

- в окне «Расширенные настройки» оставить значения по умолчанию или при необходимости изменить значения:
  - «Каталог журналов»: каталог хранения журналов для службы Агента ВРМ. Значение по умолчанию: `/var/log/termidesk`. По умолчанию после установки права на каталог соответствуют `rwxr-xr-x` (в восьмеричной записи - `755`);
  - «Каталог журналов пользователя»: каталог хранения журналов для непривилегированного пользователя. Значение по умолчанию: `~./config/UVEON/logs`;
  - «Каталог настроек»: каталог хранения конфигурационного файла. Значение по умолчанию: `/etc/termidesk`.



Окно «Расширенные настройки» будет показано единожды, если конфигурационный файл `agent.cfg` отсутствует в системе.

Предпочтительные значения в расширенных настройках будут подставлены автоматически. Если настройки были изменены, то значения подставятся с учетом их приоритета:

- в первую очередь подставляются значения из переменных окружения. Все ранее заданные значения конфигурационного файла игнорируются;
- если переменные окружения не заданы, то подставляются значения из конфигурационного файла;
- если ничего из пунктов выше не задано, то применяются значения по умолчанию.

После установки изменить настройки можно:

- через файл `/etc/default/termidesk-agent` (см. подраздел **Конфигурационные файлы Агента ВРМ**);

- через вызов программы `termidesk-agent-config`:

```
sudo termidesk-agent-config setup --dialog
```

Для «тихой» установки без отображения дополнительных окон следует назначить переменные окружения и передать их в команду установки:

```
sudo TDSK_SETUP_NONINTERACTIVE=1 TDSK_CONFIG_DIR=<путь_к_каталогу>
TDSK_LOG_SRV_DIR=<путь_к_каталогу> TDSK_LOG_USER_DIR=<путь_к_каталогу> apt install
termidesk-agent
```

где:

- `TDSK_SETUP_NONINTERACTIVE=1` - переменная, указывающая запуск в режиме «тихой» установки;
- `TDSK_CONFIG_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу с конфигурационным файлом `agent.cfg`. Например, `TDSK_CONFIG_DIR=/etc/termidesk-test`;
- `TDSK_LOG_SRV_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов службы Агента ВРМ;
- `TDSK_LOG_USER_DIR=<путь_к_каталогу>` - переменная, указывающая путь к каталогу хранения журналов для непривилегированного пользователя.

После установки нужно добавить в автоматическую загрузку и запустить службу `termidesk-agent`:

```
sudo systemctl enable termidesk-agent.service
sudo systemctl start termidesk-agent.service
```

Проверить состояние службы:

```
sudo systemctl status termidesk-agent.service
```

Обновление Агентов в других ОС Linux

Обновление Агентов выполняется установкой новой версии поверх предыдущей, кроме Агента ВРМ и Агента УВ.

Для обновления Агента ВРМ на ОС Linux нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-agent
```

- установить новую версию:

```
sudo apt install -y termidesk-agent
```

Для обновления Агента УВ нужно:

- удалить предыдущую версию (рекомендуется, чтобы корректно обновились права на каталоги для новой версии):

```
sudo aptitude purge -y termidesk-vmsd
```

- установить новую версию:

```
sudo apt install -y termidesk-vmsd
```

Удаление Агентов в других ОС Linux

Удаление Агентов выполняется командой:

```
sudo aptitude purge -y <наименование_пакета>
```

Наименования пакетов:

- `termidesk-agent` - Агент ВРМ;
- `termidesk-session-agent` - сессионный Агент;
- `termidesk-video-agent` - видеоагент;
- `termidesk-pcsc-vscard` - Агент смарт-карт;
- `termidesk-vmsd` - Агент УВ.

Если установка пакета производилась не из локального репозитория, удаление выполняется командой:

```
sudo dpkg -P <наименование_пакета>
```



Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

ОС Microsoft Windows

Установка Агента ВРМ в ОС Microsoft Windows

Для установки Агента ВРМ необходимо предварительно подготовить базовое ВРМ с гостевой ОС (см. подраздел **Обязательные настройки гостевой ОС РМ** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»).

Агент ВРМ устанавливается из `msi`-пакета `termidesk-agent`, доступного из поставляемого `iso`-образа. В состав поставляемого пакета по умолчанию включена возможность установки

подкомпонентов:

- «Temidesk PCSC Driver» - Агент смарт-карт для перенаправления подключенных к пользовательской рабочей станции смарт-карт в ВРМ;
- «Temidesk Video Agent» - видеоагент для перенаправления видеокамеры с пользовательской рабочей станции в ВРМ.

После запуска пакета необходимо:

- принять лицензионное соглашение;
- в окне «Выборочная установка» убедиться, что отмечены все компоненты, затем нажать экранную кнопку **[Далее]** (см. рисунок Окно установки компонентов Агента ВРМ).

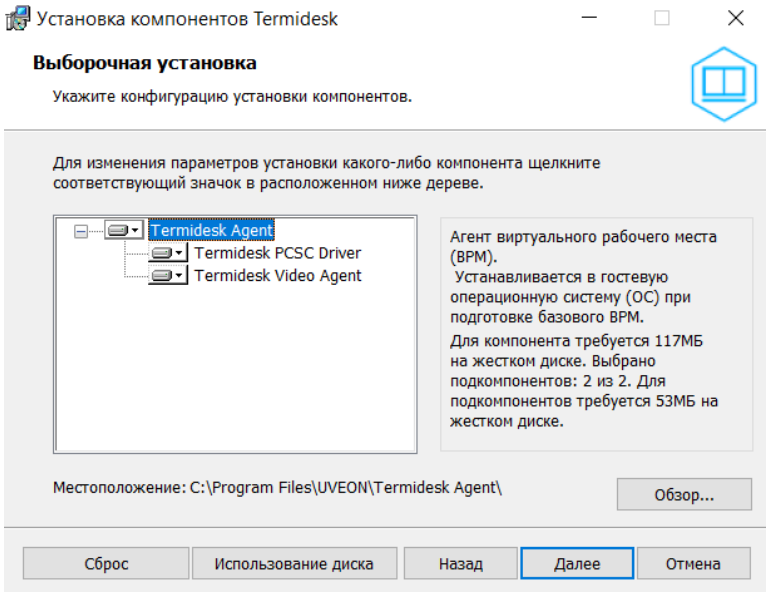


Рисунок 1. Окно установки компонентов Агента ВРМ

- в окне «Настройка редиректора WebDAV» определить максимальный размер файла для передачи через WebDAV и нажать экранную кнопку **[Далее]** (см. рисунок Окно «Настройка редиректора WebDAV»):
  - при активации пункта «Изменить ограничения по умолчанию» Агент ВРМ присваивает значение `4294967295` (4 ГБ, тип `REG_DWORD`) параметру `FileSizeLimitInBytes` в ветке реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`;
  - при отключении пункта «Изменить ограничения по умолчанию» значение параметра определяется настройками ОС Microsoft Windows (по умолчанию 50 МБ);

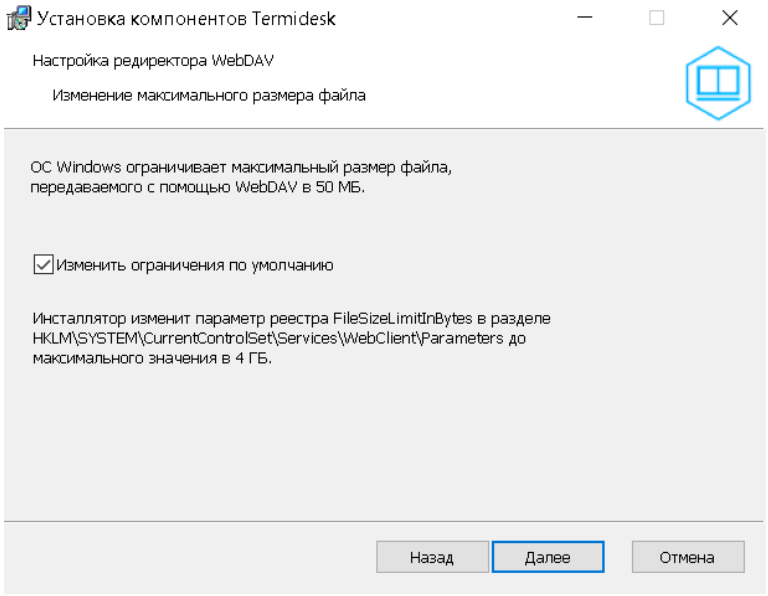


Рисунок 2. Окно «Настройка редиректора WebDAV»

- после выполнения конфигурации следует дождаться завершения установки. Установка произойдет для всех пользователей ОС;
- в окне завершения установки по умолчанию активирован параметр «Запустить мастер настройки приложения» (см. рисунок Завершение установки Агента BPM). Для перехода к настройке Агента BPM нужно нажать экранную кнопку **[Готово]** и выполнить настройку согласно подразделу **Настройка для ОС Microsoft Windows**. Для выхода из мастера установки без настройки Агента BPM нужно снять галочку в параметре «Запустить мастер настройки приложения».

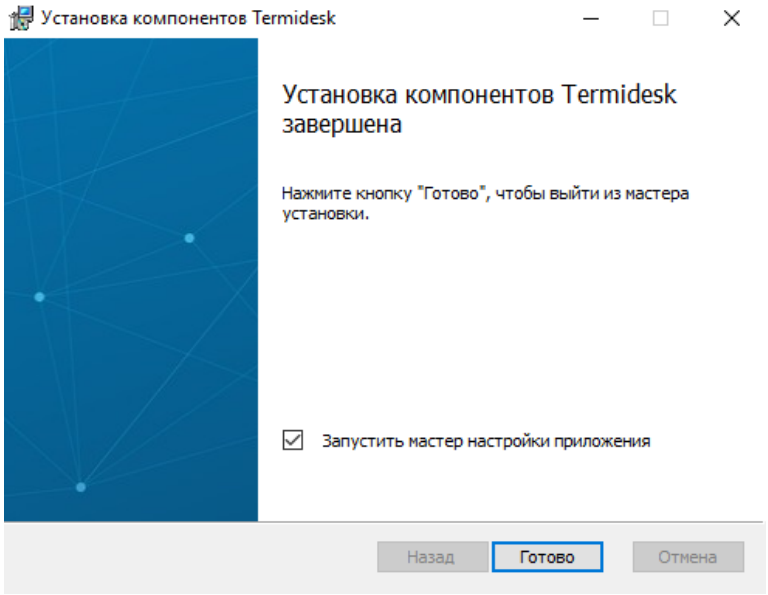


Рисунок 3. Завершение установки Агента BPM

После установки:

- будут доступны следующие службы:
  - `Termidesk Agent Daemon` - основная служба Агента BPM. Вызывается исполняемым файлом `TermideskAgentDaemon.exe`. По-умолчанию службе назначен тип запуска «Автоматически (отложенный запуск)», при котором ее запуск происходит спустя некоторое время после после запуска всех необходимых для работы служб. При ручном изменении типа запуска Агент BPM не будет его менять

в значение по-умолчанию при следующем запуске;

- `Termidesk Pcsc Rights Service` - служба, отвечающая за перенаправление подключенных к пользовательской рабочей станции смарт-карт в BPM. Вызывается исполняемым файлом `PcscRights.exe`;
- `Termidesk Video Agent` - служба, отвечающая за перенаправление видеокамеры с пользовательской рабочей станции в BPM. Вызывается исполняемым файлом `video_agent.exe`;

- будет доступно ПО tera-webdav, предоставляющее возможность перенаправления каталога из пользовательской рабочей станции в BPM. Запуск ПО tera-webdav выполняется для каждого пользователя после его авторизации в BPM с параметрами: `--no-service --rdp-enable`.

Установка Видеоагента в ОС Microsoft Windows

Видеоагент («Termidesk Video Agent») устанавливается в гостевую ОС для корректного перенаправления подключенных к пользовательской рабочей станции веб-камер и входит в состав установочного файла Агента BPM.

Установка видеоагента выполняется при установке Агента BPM (установочный файл `termidesk-agent_<версия>.msi`).

Установка Агента виртуальных смарт-карт в ОС Microsoft Windows

Агент смарт-карт («Temidesk PCSC Driver») устанавливается в гостевую ОС для корректного перенаправления подключенных к пользовательской рабочей станции смарт-карт в BPM и входит в состав установочного файла Агента BPM.

Установка Агента смарт-карт выполняется при установке Агента BPM (установочный файл `termidesk-agent_<версия>.msi`).

Установка сессионного Агента в ОС Microsoft Windows

Сессионный Агент устанавливается на сервер терминалов Microsoft Windows Server из `msi` -пакета `termidesk-session-agent`.

Для установки сессионного Агента нужно:

- выполнить запуск установочного файла `termidesk-session-agent_XXX.msi`;
- в окне приветствия нажать кнопку **[Далее]** (см. рисунок Окно приветствия установки сессионного Агента);

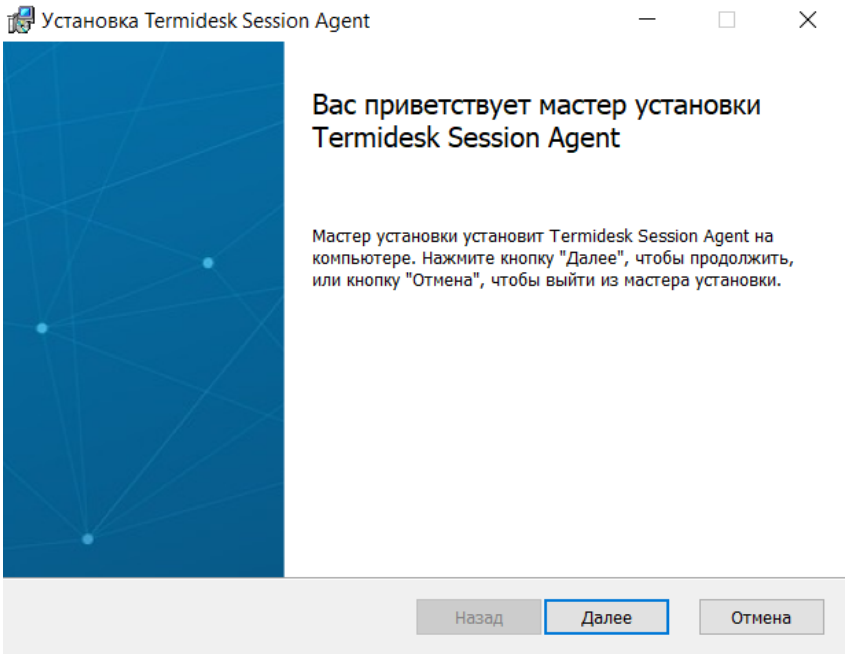


Рисунок 4. Окно приветствия установки сессионного Агента

- принять условия лицензионного соглашения и нажать кнопку **[Далее]** (см. рисунок Окно с условиями лицензионного соглашения);

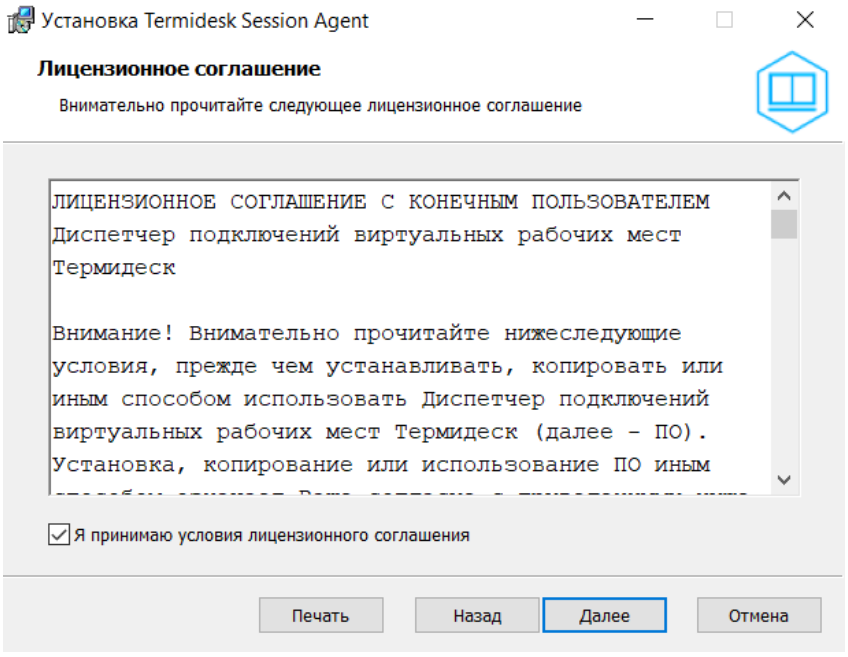


Рисунок 5. Окно с условиями лицензионного соглашения

- выбрать путь установки или оставить его по умолчанию и нажать кнопку **[Далее]** (см. рисунок Окно выбора каталога установки);

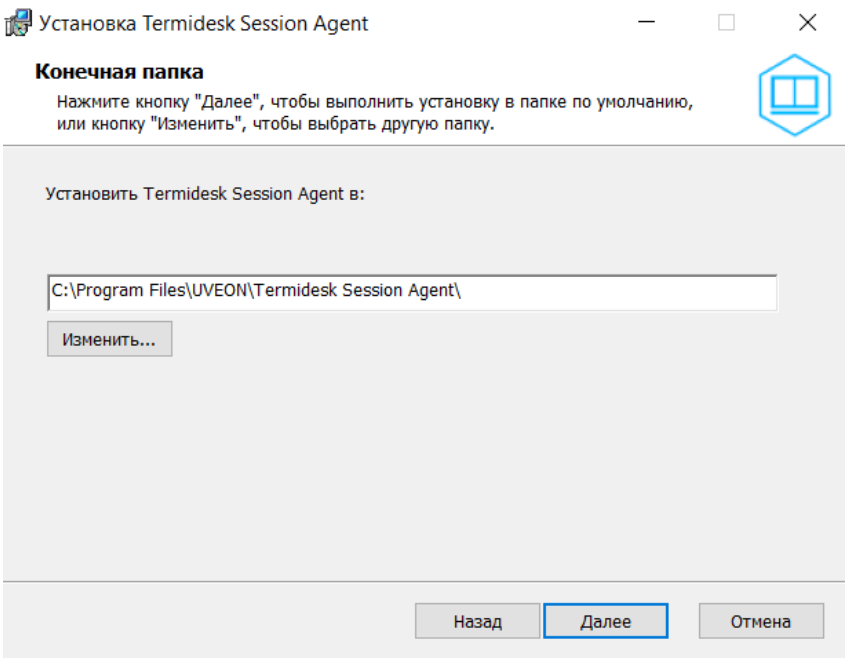


Рисунок 6. Окно выбора каталога установки

- нажать кнопку **[Установить]** для начала процесса установки (см. рисунок Окно подтверждения установки);

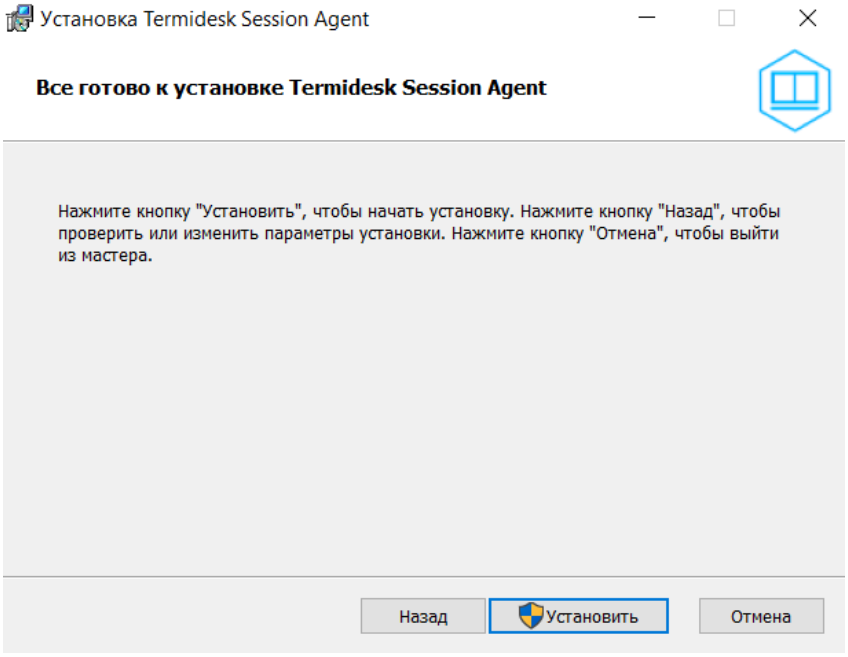


Рисунок 7. Окно подтверждения установки

- завершить работу мастера после установки сессионного Агента, нажав кнопку **[Готово]** (см. рисунок Окно подтверждения перезагрузки системы после установки);
- при появлении сообщения о необходимости перезагрузки нужно согласиться с перезагрузкой системы, нажав кнопку **[ОК]** (см. рисунок Окно подтверждения перезагрузки системы после установки). В противном случае установка будет прервана.

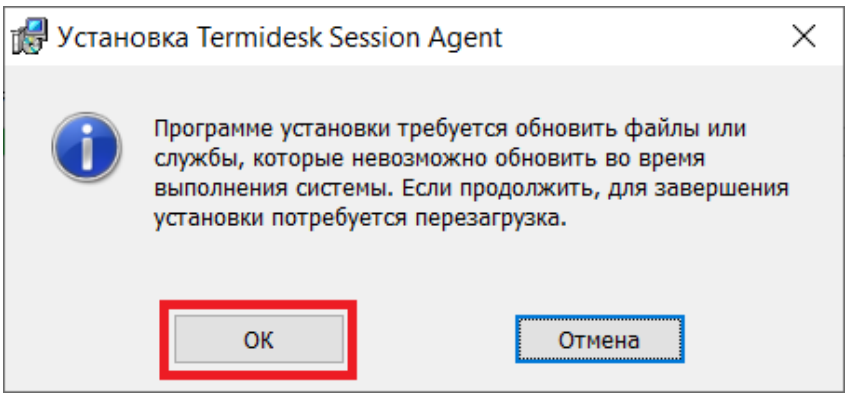


Рисунок 8. Окно подтверждения перезагрузки системы после установки

После установки создастся конфигурационный файл `C:\ProgramData\UVEON\Termidesk Session Agent\session_agent.ini`.

После установки сессионного Агента:

- необходимо создать правило для брандмауэра на открытие порта `31000`;
- при необходимости может быть выполнена настройка согласно подразделу **Первичная настройка**;
- будет создан файл базы данных (БД) SQLite `C:\ProgramData\UVEON\Termidesk Session Agent\log\termidesk_ssa.db`, который предназначен для сбора и хранения метрик узла. БД инициализируется при запуске сессионного Агента.

Установка Агента BPM через интерфейс командной строки

Для выполнения тихой установки (silent install) Агента BPM через командную строку `cmd.exe` нужно:

- открыть интерфейс командной строки от имени администратора;
- выполнить команду `msiexec`:

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" /qn
```

Где:

`/qn` - обеспечивает тихую установку, без отображения окон и сообщений.

По умолчанию вместе с Агентом BPM будут установлены Агент смарт-карт («Temidesk PCSC Driver») и видеоагент («Temidesk Video Agent»). Для управления установкой компонентов нужно воспользоваться свойством ADDLOCAL:

- команда установки только Агента BPM (при этом другие компоненты установлены не будут):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_Agent" /qn
```

- команда установки только Агента смарт-карт (при этом Агент BPM все равно будет установлен):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_PCSC_Driver"
/qn
```

- команда установки только видеоагента (при этом Агент ВРМ все равно будет установлен):

```
msiexec /i "<путь_к_пакету_termidesk-agent>.msi" ADDLOCAL="Termidesk_Video_Agent"
/qn
```

При установке Агента ВРМ может быть задан максимальный размер файла, передаваемого через WebDAV. Для управления конфигурацией следует воспользоваться свойством `WEBDAVFILESIZELIMITINBYTES` с нужным значением:

- `1` - присваивает значение `4294967295` (4 ГБ, тип `REG_DWORD`) параметру `FileSizeLimitInBytes` в ветке реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`;
- `0` - устанавливает параметр `FileSizeLimitInBytes` в исходное значение ОС Microsoft Windows - `52428800` (50 МБ).

Сценарии установки:

- первая установка в тихом режиме. При первой установке Агента ВРМ без свойства `WEBDAVFILESIZELIMITINBYTES` будет применено значение по умолчанию - `0` (максимальный размер файла определяется ОС Microsoft Windows - 50 МБ);
- установка поверх предыдущей версии:
  - если ранее Агент ВРМ был установлен со свойством `WEBDAVFILESIZELIMITINBYTES=0` или без него и необходимо изменить конфигурацию, то выполнить, используя ту же версию пакета:

    ```
    msiexec /i "<путь_к_пакету_termidesk-agent>.msi" WEBDAVFILESIZELIMITINBYTES=1
    /qn
    ```

  - если ранее Агент ВРМ был установлен со свойством `WEBDAVFILESIZELIMITINBYTES=1` и необходимо изменить конфигурацию, то выполнить, используя ту же версию пакета:

    ```
    msiexec /i "<путь_к_пакету_termidesk-agent>.msi" WEBDAVFILESIZELIMITINBYTES=0
    /qn
    ```

Обновление Агентов в ОС Microsoft Windows

Обновление Агентов выполняется установкой новой версии поверх предыдущей.

В случае, если обновление компонента «Универсального диспетчера» произошло раньше обновления сессионного Агента, то на узле с «Универсальным диспетчером» (роль «Портал администратора») нужно:

- в интерфейсе командной строки переключиться на пользователя `termidesk`:

```
sudo -u termidesk bash
```

- выполнить регистрацию сессионного Агента:

```
/opt/termidesk/sbin/termidesk-vdi-manage tdsk_refresh_ssa
```

Удаление Агентов в ОС Microsoft Windows

Удаление Агентов из среды ОС Microsoft Windows выполняется через «Пуск - Панель управления - Удаление программы». Необходимо выбрать из списка установленных программ компонент и нажать экранную кнопку **[Удалить]**.



При удалении Агента восстанавливается исходное значение параметра `FileSizeLimitInBytes` в ветви реестра `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WebClient\Parameters`.



Вместе с удалением сессионного Агента будет удален файл БД SQLite `termidesk_ssa.db`.

АГЕНТ. НАСТРОЙКИ

Переменные окружения и аргументы командной строки

Переменные окружения и другие параметры конфигурирования

В Termidesk VDI используются переменные окружения для указания параметров настройки компонентов программного комплекса.

Для включения переопределения значений параметров Агента ВРМ через переменные окружения используются два способа:

- активация параметра «Разрешить переопределение значений через переменные окружения» в графическом интерфейсе Агента ВРМ. Для ОС Linux должен быть задан файл с перечислением переменных окружения и их значениями `/etc/default/termidesk-agent`;
- или назначение параметру `env` значения `True` в конфигурационном файле `/etc/termidesk/agent.cfg`. Для ОС Linux должен быть задан файл с перечислением переменных окружения и их значениями `/etc/default/termidesk-agent`.

Для других Агентов дополнительные действия не требуются.

В ОС Microsoft Windows задание настроек Агента ВРМ может быть выполнено из командной строки. Для этого:

- открыть командную строку от имени администратора;
- вызывать Агент ВРМ из каталога `C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe`;
- выполнить:

```
"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --host
192.0.2.30 --key 0123456789 --loglevel 20000 --httpd-port=43900
```

где:

`--host 192.0.2.30` - IP-адрес компонента «Универсальный диспетчер» («Портала администратора»);

`--key 0123456789` - значение мастер-ключа для подключения к компоненту «Универсальный диспетчер» («Порталу администратора»);

`--loglevel 20000` - категория сообщений;

`--httpd-port=43900` - порт Агента ВРМ.

Пример получения полной информации по доступным аргументам командной строки с выводом в файл `C:\agent_help_all.txt`:

```
"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" -h >
C:\agent_help_all.txt
```

Агент ВРМ также предусматривает возможность конфигурирования переносимых профилей и настройки аутентификации пользователей ВРМ через файл с помощью модуля `pam_tdsk`. Для подробной информации следует обратиться к подразделам **Перемещаемые**

профили, **Технология единого входа**, **Настройка аутентификации пользователей BPM через файл**документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса».

Перечень переменных окружения и аргументов CLI, используемых Агентами, приведены далее в таблицах:

- переменные окружения Агента BPM (см. таблицу Переменные окружения и аргументы CLI Агента BPM);
- переменные окружения Агента УВ (см. таблицу Переменные окружения Агента УВ);
- переменные окружения видеоагента (см. таблицу Переменные окружения и аргументы CLI видеоагента);
- переменные окружения Агента смарт-карт (см. таблицу Переменные окружения Агента смарт-карт);
- переменные окружения сессионного Агента (см. таблицу Переменные окружения сессионного Агента).

Таблица 3. Переменные окружения и аргументы CLI Агента BPM

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_AD_JOIN_METHOD	Не задано	Управляет способом ввода BPM в домен MS AD. Переменная окружения используется только в ОС Linux. Возможные значения: • adcli - ввод BPM в домен MS AD с использованием утилиты adcli; • samba - ввод BPM в домен MS AD с использованием средств пакета samba	Не задано
TDSK_VDI_URL	Не задано	Задает URL-адрес компонента «Универсальный диспетчер» («Портала администратора») для подключения к нему	--host
TDSK_VDI_KEY	Не задано	Задает значение мастер-ключа для подключения к компоненту «Универсальный диспетчер» («Порталу администратора»). Для получения значения мастер-ключа в «Портале администратора» нужно перейти «Системные параметры - Системные настройки - Безопасность»	--key

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки

TDSK_VDI_LOGLEVEL	20000	Задает категорию сообщений, которые будут записываться в журнал Агента BPM.
		
		Возможные значения (может указываться как цифровое значение, так и буквенное):
		
		• 20000 - соответствует уровню DEBUG;
		• 30000 - соответствует уровню INFO;
		• 40000 - соответствует уровню WARN;
		• 30000 - соответствует уровню ERROR;
		• 40000 - соответствует уровню FATAL.
		
		Пример для ОС Linux:
		
		`sudo termidesk-agent-config update --loglevel 20000`
		`sudo termidesk-agent-config update --loglevel INFO`
		
		Пример для ОС Microsoft Windows:
		
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --loglevel 20000`
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --loglevel INFO`
			--loglevel

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки

Не задано	Не задано	Управление режимом подстановки значений параметров из переменных окружения.
		
		Возможные значения:
		
		• True - использовать подстановку значений параметров из переменных окружения;
		• False - не использовать подстановку значений параметров из переменных окружения.
		
		Если не задать значение, то будет использоваться True.
		
		Пример для ОС Linux:
		
		`sudo termidesk-agent-config update --env=True`
		`sudo termidesk-agent-config update --env`
		
		Пример для ОС Microsoft Windows:
		
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --env=True`
		`"C:\Program Files\UVEON\Termidesk Agent\TermideskAgentConfig.exe" update --env`
			--env

TDSK_METRIC_INTERVAL	3	Интервал (в секундах) получения и обновления метрик узла Агентом ВРМ. Переменная окружения доступна с версии 5.1. По умолчанию интервал 3 секунды, однако через REST API получить метрики можно в любой момент	Не задано
SSSD_DEFAULT_CONF	/etc/sssd/sssd.conf	Задает путь к конфигурационному файлу, в котором задано значение параметра use_fully_qualified_names. В зависимости от значения параметра use_fully_qualified_names будут применены действия: • суффикс домена не будет подставлен, если use_fully_qualified_names = False или отсутствует; • суффикс домена будет подставлен, если use_fully_qualified_names = True	Не задано
TDSK_LOG_ROTATE_COUNT	5	Задает максимальное количество файлов журналов. Переменная окружения доступна с версии 6.0	Не задано

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_LOG_ROTATE_MAX_SIZE	10	Задает максимальный размер (МБ) файла журнала. Переменная окружения доступна с версии 6.0	Не задано
LOUDPLAY_LISTEN_IPV4	127.0.0.1	Задает IP-адрес сервера Loudplay для взаимодействия с ним	Не задано
LOUDPLAY_LISTEN_PORT	10061	Задает порт сервера Loudplay для взаимодействия с ним	Не задано
LOUDPLAY_CONNECT_DELAY	30	Задает время ожидания (в секундах), по истечении которого Агент ВРМ отключит неактивную сессию пользователя на сервере Loudplay	Не задано

TDSK_CONFIG_DIR	Не задано	Задает место хранения файлов конфигурации Агента ВРМ.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования Агента ВРМ.
		
		Для этого ему нужно:
		
		• создать файл agent.cfg с настройками или скопировать его из /etc/termidesk;
		• поместить agent.cfg в нужный каталог. Каталог должен обладать свойствами:
		  права доступа: rw-r--r-- (в восьмеричной записи - 644);
		  владелец и группа: root:root;
		• создать файл /etc/default/termidesk-agent. Указать в нем каталог, откуда будет считан конфигурационный файл:
		
		`TDSK_CONFIG_DIR=/etc/opt/termidesk`
		
		• перезапустить службу termidesk-agent:
		
		`sudo systemctl restart termidesk-agent`
			Не задано

TDSK_HTTP_PORT	43900	Сетевой порт HTTP-сервера Агента ВРМ. Начиная с Termidesk VDI версии 6.1 для работы Агента ВРМ более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задаются вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535	--httpd-port

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_HTTP_INTERFACE	Не задано	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». Переменная окружения доступна с версии 7.0. В качестве значения используется наименование сетевого интерфейса. Пример для ОС Linux: `Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически`	Не задано
TDSK_LOG_SRV_DIR	Не задано	Каталог хранения журналов службы Агента ВРМ	Не задано
TDSK_LOG_USER_DIR	Не задано	Каталог хранения журналов для непривилегированного пользователя	Не задано
TDSK_SETUP_NONINTERACTIVE	Не задано	«Тихий» режим установки. Возможные значения: • 1 - активировать режим. Используется при необходимости установки Агента ВРМ без отображения дополнительных окон	Не задано
TERA_QXL_CONFIG_FILE	Не задано	Путь к конфигурационному файлу TERA для ВМ. Используется для считывания параметров, заданных в настройках TERA. Если значение не задано, то используется путь /etc/X11/xorg.conf.d/30-teraqxl.xorg.conf	Не задано
TDSK_SSO_WAITING_TIMEOUT	60	Время (в секундах) задержки подключения ПО Termidesk Viewer к РМ при использовании технологии единого входа (SSO). Переменная ограничивает время, по истечении которого Агент ВРМ уведомит компонент «Клиент» о неудачной процедуре SSO. Значение менять не рекомендуется: при штатном сценарии вход в систему выполняется быстрее установленного лимита. Изменение значения может потребоваться только в случаях отладки и при возникновении проблем с подключением	Не задано

Таблица 4. Переменные окружения Агента УВ

Переменная окружения	Значение по умолчанию	Описание

TVMD_ILEVEL_SOCKET	63	Задает значение метки целостности на создаваемый TVMD -сокет. Параметр задается в конфигурационном файле /etc/termidesk/termidesk-vmsd.conf.
		
		По умолчанию после установки конфигурационный файл может не существовать. В этом случае нужно:
		
		• создать каталог /etc/termidesk/:
		
		`sudo mkdir /etc/termidesk`
		
		• изменить права на каталог:
		
		`sudo chmod 755 /etc/termidesk`
		
		• создать конфигурационный файл:
		
		`sudo touch /etc/termidesk/termidesk-vmsd.conf`
		
		• изменить права на файл:
		
		`sudo chmod 644 /etc/termidesk/termidesk-vmsd.conf`
		
		Изменение значения метки целостности может понадобиться, если ОС имеет уровень целостности, отличный от 16. При возникновении ситуации, когда уровень целостности ОС отличается от 16, следует:
		
		• узнать текущий уровень целостности, выставляемый ОС для ВМ, командой:
		
		`cat /etc/libvirt/libvirtd.conf | grep ilev_vm`
		
		• если полученный уровень отличается, то добавить параметр TVMD_ILEVEL_SOCKET с нужным значением уровня (например,TVMD_ILEVEL_SOCKET=16) в конфигурационный файл /etc/termidesk/termidesk-vmsd.conf

LIBVIRT_PASSWORD_SCRIPT	Не задано	Задает путь для исполняемого файла, реализующего альтернативный механизм сброса сессий (см. подраздел **Использование альтернативного механизма сброса сессий**)

Таблица 5. Переменные окружения и аргументы CLI видеоагента

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
TDSK_DEBUG	Не задано	Включение режима отладки. Возможные значения: yes	Не задано

Переменная окружения	Значение по умолчанию	Описание	Аргумент командной строки
Не задано	Не задано	Вывод справки по использованию аргументов командной строки. Для вызова справки нужно выполнить: `sudo /usr/local/sbin/video_agent -h`	-h
Не задано	/dev/video0	Устройство вывода видео	-o
Не задано	Не задано	Вывод версии приложения. Для вывода версии нужно выполнить: `sudo /usr/local/sbin/video_agent -v`	-v
TDSK_VIDEO_CODEC	libtheora	Кодек видеокамеры. Возможные значения: • libtheora - нативный метод кодирования Theora; • theora - кодирование через конвейер Gstreamer	-c

Таблица 6. Переменные окружения Агента смарт-карт

Переменная окружения	Значение по умолчанию	Описание
TDSK_DEBUG	Не задано	Включение режима отладки. Может также использоваться файл /etc/reader.conf.d/exconf/vscard (см. подраздел **Настройка Агента виртуальных смарт-карт**). Возможные значения: yes

Таблица 7. Переменные окружения сессионного Агента

Переменная окружения	Значение по умолчанию	Описание

CONFIG_DIR	/etc/opt/termidesk-session-agent	Задает каталог хранения конфигурационных файлов сессионного Агента.
		
		Пример: администратор хочет изменить место хранения файла конфигурирования сессионного Агента.
		
		Для этого нужно:
		
		• создать файл session_agent.ini с настройками или скопировать его из существующего каталога;
		• поместить session_agent.ini в нужный каталог. Каталог должен обладать свойствами:
		  права доступа: rwxr-xr-x (в восьмеричной записи - 755);
		  владелец и группа: termidesk:termidesk;
		• создать файл /etc/default/termidesk-session-agent (если он не существует). Указать в нем каталог в переменной CONFIG_DIR, откуда будет считан конфигурационный файл. Пример:
		
		`CONFIG_DIR=/etc/opt/termidesk/session-agent`
		
		• перезапустить службу termidesk-session-agent.service:
		
		`sudo systemctl restart termidesk-session-agent.service`

Агент BPM

Конфигурационные файлы Агента BPM

Конфигурационный файл Агента BPM

Для настройки Агента BPM используется конфигурационный файл:

- в ОС Linux - /etc/termidesk/agent.cfg;



Администратор может изменить каталог хранения файла в ОС Linux на этапе установки или через переменную окружения TDSK_CONFIG_DIR, указанную в файле /etc/default/termidesk-agent.

- в ОС Microsoft Windows - конфигурационный файл упакован и размещен в реестре по пути HKEY_LOCAL_MACHINE\Software\Termidesk\Agent.

Параметры, доступные в конфигурационном файле для ОС Linux, приведены в таблице (см. таблицу Параметры конфигурирования Агента BPM в ОС Linux).

Таблица 8. Параметры конфигурирования Агента BPM в ОС Linux

Параметр	Значение по умолчанию	Описание
Секция [agent]		
adJoinMethod	Не задано	Управление способом ввода ВРМ в домен MS AD. Возможные значения: • adcli - ввод ВРМ в домен MS AD с использованием утилиты adcli; • samba - ввод ВРМ в домен MS AD с использованием средств пакета samba
env	False	Управление режимом переопределения параметров через переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**). Для ОС Linux должен быть задан файл /etc/default/termidesk-agent с перечислением переменных окружения и их значениями (см. подраздел **Конфигурационные файлы Агента ВРМ**). Возможные значения: • True - режим включен. Значения параметров переопределяются через переменные окружения; • False - режим отключен
host	Не задано	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портала администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/host
hostSSL	ssl_host	SSL-профиль (настройки SSL) для HTTP-клиента. Профиль задается ниже в секции [ssl_host]. Может быть задано несколько SSL-профилей
httpSSL	ssl_http	SSL-профиль для HTTP-сервера. Профиль задается ниже в секции [ssl_http]. Может быть задано несколько SSL-профилей
httpSSLasHost	False	Управление режимом использования SSL-профиля HTTP-сервера для запросов к компоненту «Универсальный диспетчер». Возможные значения: • True - использовать SSL-профиль HTTP-сервера для запросов к компоненту «Универсальный диспетчер»; • False - не использовать SSL-профиль HTTP-сервера для запросов к компоненту «Универсальный диспетчер»

Параметр	Значение по умолчанию	Описание
`httpPort`	`43900`	Сетевой порт HTTP-сервера Агента ВРМ. Начиная с Termidesk VDI версии 6.1 для работы Агента ВРМ более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задается вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535
`httpInterface`	`Не задано`	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда РМ. В качестве значения используется наименование сетевого интерфейса. Пример использования: `httpInterface = enp6s0` Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически
`vault`	`vault_host`	Профиль защищенного хранилища секретов. Параметры профиля задаются в секции `[vault_host]`. Может быть задано несколько профилей защищенного хранилища секретов
`metrics`	`metrics_host`	Профиль хранения метрик. Параметры профиля задаются в секции `[metrics_host]`
`masterKey`	`Не задано`	Значение мастер-ключа для подключения к компоненту «Универсальный диспетчер». Для получения значения мастер-ключа нужно перейти в «Портале администратора»: «Системные параметры - Системные настройки - Безопасность». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
`logLevel`	`20000`	Степень детализации служебных сообщений. Возможные значения: • `20000` - соответствует уровню DEBUG; • `30000` - соответствует уровню INFO; • `40000` - соответствует уровню WARN; • `50000` - соответствует уровню ERROR; • `60000` - соответствует уровню FATAL

Параметр	Значение по умолчанию	Описание
logoffSignal	0	Управление сигналом завершения сессии через утилиту loginctl. WARNING: Значение параметра применяется только к новым сессиям и не влияет на активные сессии. При значении 0 по умолчанию используется сигнал SIGTERM (15). Возможные значения: от 0 до 33
logSrvDir	/var/log/termidesk	Каталог хранения журналов службы Агента BPM. По умолчанию после установки права на каталог соответствуют rwxr-xr-x (в восьмеричной записи - 755)
logUserDir	~/config/UVEON/logs	Каталог хранения журналов для непривилегированного пользователя
mtls	DISABLED	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • DISABLED (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент BPM использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется; • PERMISSIVE - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • STRICT - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
certSource	Не задано	Тип хранилища сертификатов. Возможные значения: • FILESYSTEM - сертификаты располагаются локально, в файловой системе; • VAULT - сертификаты располагаются во внешнем защищенном хранилище сертификатов
ssl	True	Управление режимом подключения к компоненту «Универсальный диспетчер». Начиная с Termidesk 6.1 подключение всегда выполняется по протоколу HTTPS. Менять значение не рекомендуется
rebootAfterOperation	True	Необходимость перезагрузки ОС, если узел переименуется. Параметр действует только в ОС Linux. Возможные значения: • True - ОС будет перезагружена, если узел переименуется; • False - ОС не будет перезагружена
Секция [ssl_host]		

Параметр	Значение по умолчанию	Описание
`ca`	`Не задано`	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
`certificate`	`Не задано`	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
`certificateKey`	`Не задано`	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
`passphrase`	`Не задано`	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
		Секция `[ssl_http]`
`ca`	`Не задано`	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM

Параметр	Значение по умолчанию	Описание
certificate	Не задано	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
certificateKey	Не задано	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
passphrase	Не задано	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Секция [vault_host]		
role_id	Не задано	Идентификатор роли, используемый для взаимодействия с защищенным хранилищем секретов
ttl	3600	Время (в секундах) жизни токена, использующегося для аутентификации при подключении к защищенному хранилищу секретов
ttl_deadline	30	Оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен
timeout	1	Время ожидания (в секундах) подключения к защищенному хранилищу секретов
token	Не задано	Путь к файлу с токеном подключения к защищенному хранилищу секретов
url	Не задано	URL-адрес подключения к защищенному хранилищу секретов
Секция [metrics_host]		
interval	3	Периодичность (в секундах) опроса и сохранения метрик сессий
filepath	Не задано	Путь к файлу хранения сведений о метриках сессий. Если значение не задано, то используется /var/lib/termidesk/agent/metrics.json

Параметры, доступные для ОС Microsoft Windows, приведены в таблице (см. таблицу Параметры конфигурирования Агента BPM в ОС Microsoft Windows).

Таблица 9. Параметры конфигурирования Агента BPM в ОС Microsoft Windows

Параметр	Тип	Описание
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Policies		

Параметр	Тип	Описание
HKLMReboot	dword	Параметр определяет необходимость перезагрузки ОС после изменения реестра ОС. Возможные значения: • 00000000 - если политики реестра изменились, ОС не будет перезагружена; • 00000001 - если политики реестра изменились, ОС будет перезагружена. Если параметр отсутствует, то: • для Агента ВРМ версии ниже 6.1 ОС будет перезагружаться после обновления реестра; • для Агента ВРМ версии 6.1 и выше ОС не будет перезагружаться после обновления реестра

PrinterRedirectPolicy	dword	Параметр определяет работу функционала перенаправления принтеров на стороне Агента ВРМ.
		
		Возможные значения:
		
		• 00000000 - перенаправление принтеров запрещено;
		• 00000001 - перенаправление принтеров разрешено.
		
		Значение по умолчанию: 00000001.
		
		Особенности работы:
		
		• Агент ВРМ при создании РМ вне зависимости от политики Termidesk VDI записывает значение в реестр:
		  00000000 (разрешить перенаправление) в HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDisableCpm;
		  00000001 (разрешить перенаправление) в HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Policies;
		• после применения значения Агент ВРМ перегружает РМ;
		• Агент ВРМ отслеживает значение параметра реестра fDisableCpm. Если оно изменилось, то Агент ВРМ фиксирует событие изменения в журнале РМ, не пытаясь обновить реестр

Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store		
env	dword	Управление режимом переопределения параметров через переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**). Возможные значения: • 1 - режим включен. Значения параметров переопределяются через переменные окружения; • 0 (по умолчанию) - режим отключен
host	sz	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портала администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/host

Параметр	Тип	Описание
`httpInterface`	`sz`	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер». IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда РМ. В качестве значения используется наименование сетевого интерфейса. Если значение не задано, либо указанный интерфейс отсутствует, то выбор сетевого интерфейса выполняется автоматически
`httpPort`	`dword`	Сетевой порт HTTP-сервера Агента ВРМ. Начиная с Termidesk версии 6.1 для работы Агента ВРМ более не выбираются случайные RPC-порты из диапазона 43900-44000. Теперь порт задается вручную через конфигурационный файл или через переменную окружения. Если порт не задан, то используется значение по умолчанию. Возможные значения: от 1 до 65535 Значение по умолчанию: 43900
`logLevel`	`sz`	Степень детализации служебных сообщений. Возможные значения: • `DEBUG`; • `INFO`; • `WARN`; • `ERROR`; • `FATAL`
`masterKey`	`sz`	Значение мастер-ключа для подключения к компоненту «Универсальный диспетчер». Для получения значения мастер-ключа нужно перейти в «Портале администратора»: «Системные параметры - Системные настройки - Безопасность». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
`modifyTimeStamp`	`dword`	Время Unix последнего изменения конфигурации Агента ВРМ

Параметр	Тип	Описание
mtls	sz	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • DISABLED (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент BPM использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется; • PERMISSIVE - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • STRICT - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\ssl_host		
ca	sz	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
certificate	sz	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
certificateKey	sz	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
MSx509Location	sz	Область хранилища сертификатов ОС Microsoft Windows. Возможные значения: • MACHINE - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в HKEY_LOCAL_MACHINE; • USER - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в HKEY_CURRENT_USER
MSx509Use	sz	Отпечаток сертификата, выбранного в хранилище сертификатов ОС Microsoft Windows

Параметр	Тип	Описание
passphrase	sz	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\ssl_http		
ca	sz	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
certificate	sz	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}.com#example-dot-com/certificate В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
certificateKey	sz	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key В параметре поддерживается использование значения {{fqdn}}. При обработке пути Агент BPM автоматически заменяет значение {{fqdn}} на FQDN PM. Также допускается ручное указание FQDN PM
MSx509Location	sz	Область хранилища сертификатов ОС Microsoft Windows. Возможные значения: • MACHINE - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в HKEY_LOCAL_MACHINE; • USER - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в HKEY_CURRENT_USER
MSx509Use	sz	Отпечаток сертификата, выбранного в хранилище сертификатов ОС Microsoft Windows
passphrase	sz	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: hvac-kv://secret#agent/passphrase
Каталог реестра HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\vault_host		
role_id	sz	Идентификатор роли, используемый для взаимодействия с защищенным хранилищем секретов

Параметр	Тип	Описание
timeout	dword	Время ожидания (в секундах) подключения к защищенному хранилищу секретов
token	sz	Путь к файлу с токеном подключения к защищенному хранилищу секретов
ttl	dword	Время (в секундах) жизни токена, использующегося для аутентификации при подключении к защищенному хранилищу секретов
url	sz	URL-адрес подключения к защищенному хранилищу секретов
ttl_deadline	dword	Оставшееся время (в секундах) актуальности токена, по достижении которого он будет обновлен

Файл /etc/default/termidesk-agent

Одним из параметров службы termidesk-agent является аргумент EnvironmentFile, задающий путь к дополнительным аргументам запуска, перечисленным в файле /etc/default/termidesk-agent.

Файл /etc/default/termidesk-agent:

- является необязательным и может отсутствовать в ОС;
- если он существует, то происходит его построчное чтение в формате <ключ>=<значение> и в запускаемый процесс Агента ВРМ добавляются переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**).

Настройка для ОС Astra Linux Special Edition

Настройка Агента ВРМ для ОС Astra Linux Special Edition 1.7

Для настройки Агента ВРМ нужно:

- перейти в графическом интерфейсе ОС в «Звезда - Панель управления - Система» и выбрать ярлык «VDI Agent Configuration» (см. рисунок Расположение ярлыка Агента ВРМ в ОС);

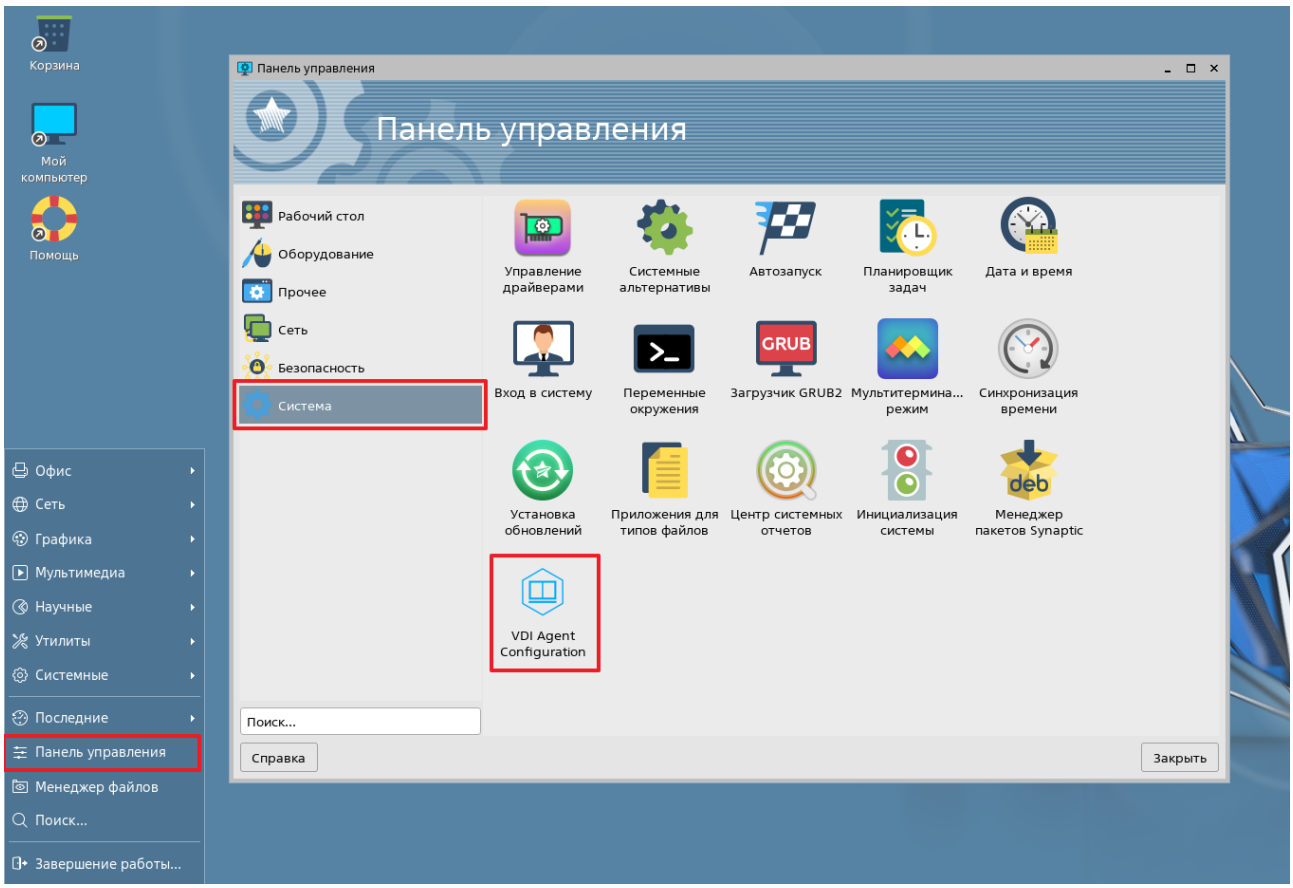


Рисунок 9. Расположение ярлыка Агента ВРМ в ОС

- ввести пароль суперпользователя ОС;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.7);
- при использовании защищенного хранилища секретов нужно задать параметры подключения к нему в конфигурационном файле `/etc/termidesk/agent.cfg` (см. подраздел **Конфигурационный файл Агента ВРМ**).

Таблица 10. Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.7

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`

Параметр	Описание
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»
«Порт агента»	Порт, на котором Агент BPM будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер».  IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда BPM.  Начиная с Termidesk VDI версии 6.1 Агент BPM подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента BPM через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)

Параметр	Описание
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент BPM использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM

Параметр	Описание
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM

Параметр	Описание
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.



Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован (см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.

Настройка Агента ВРМ для ОС Astra Linux Special Edition 1.8

Для настройки Агента ВРМ нужно:

- перейти в графическом интерфейсе ОС в «Звезда - Программы - Инструменты» и выбрать ярлык «VDI Agent Configuration» (см. рисунок Расположение ярлыка Агента ВРМ в ОС);

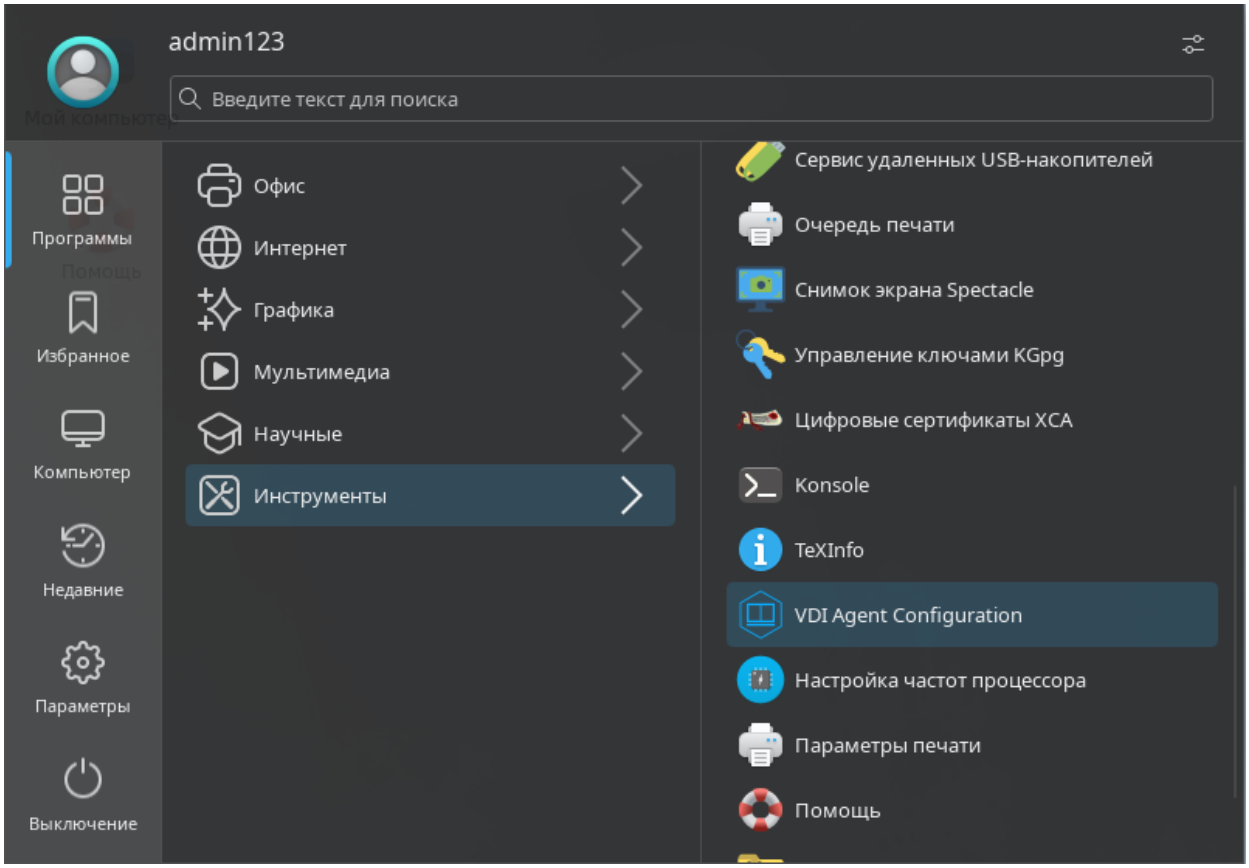


Рисунок 10. Расположение ярлыка Агента ВРМ в ОС

- ввести пароль суперпользователя ОС;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.8);
- при использовании защищенного хранилища секретов нужно задать параметры подключения к нему в конфигурационном файле `/etc/termidesk/agent.cfg` (см. подраздел **Конфигурационный файл Агента ВРМ**).

Таблица 11. Основные параметры конфигурирования Агента ВРМ в ОС Astra Linux Special Edition 1.8

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`

Параметр	Описание
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»
«Порт агента»	Порт, на котором Агент BPM будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер».  IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда BPM.  Начиная с Termidesk VDI версии 6.1 Агент BPM подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента BPM через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)

Параметр	Описание
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент BPM использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM

Параметр	Описание
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM

Параметр	Описание
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.



Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован (см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.

Настройка для ОС Microsoft Windows

Настройка Агента ВРМ для ОС Microsoft Windows

После установки Агента ВРМ следует выполнить его настройку для взаимодействия с компонентом «Универсальный диспетчер».

Для настройки Агента ВРМ нужно:

- перейти «Пуск - Все программы» выбрать каталог «Termidesk» и нажать левой клавишей мыши на ярлык Агента «Termidesk VDI Agent»;
- указать основные параметры конфигурирования (см. таблицу Основные параметры конфигурирования Агента ВРМ в ОС Microsoft Windows);
- при использовании защищенного хранилища секретов задать параметры подключения к нему в каталоге реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Agent\Store\vault_host` (см. подраздел **Конфигурационный файл Агента ВРМ**).



Начиная с Termidesk VDI версии 5.0 запускать ярлык Агента «Termidesk Agent» от имени администратора вручную не требуется, если в ОС включен контроль учетных записей пользователя (User Account Control, UAC). В случае, если контроль учетных записей выключен, то для пользователя, не являющегося администратором, появится сообщение «Эта программа должна запускаться от привилегированного пользователя», а не окно ввода данных привилегированного пользователя.

Таблица 12. Основные параметры конфигурирования Агента ВРМ в ОС Microsoft Windows

Параметр	Описание
«Адрес сервера»	IP-адрес или FQDN компонента «Универсальный диспетчер» («Портал администратора»). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/host`
«Мастер-ключ»	Используется для взаимодействия с компонентом «Универсальный диспетчер». Значение мастер-ключа можно получить в «Портале администратора», перейдя в «Системные параметры - Системные настройки - Безопасность» и скопировав значение параметра «Мастер-ключ». Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/masterKey`

Параметр	Описание
«Уровень отладки»	Степень детализации служебных сообщений. Возможные значения: • «DEBUG»; • «INFO» (по умолчанию); • «WARN»; • «ERROR»; • «FATAL»
«Порт агента»	Порт, на котором Агент BPM будет принимать подключения от компонента «Универсальный диспетчер». Если номер порта не задан, то при проверке корректности параметров будет восстановлено значение по умолчанию («43900»)
«Сетевой интерфейс»	Сетевой интерфейс, используемый для подключения к компоненту «Универсальный диспетчер».  IP-адреса выбранного интерфейса должны находиться в маршрутизируемой сети и быть доступны компоненту «Универсальный диспетчер» после публикации фонда BPM.  Начиная с Termidesk VDI версии 6.1 Агент BPM подключается к «Универсальному диспетчеру» («Порталу администратора») только по защищенному соединению (протоколу HTTPS). Если значение не задано, либо указанный интерфейс отсутствует, то будет восстановлено значение по умолчанию («Автоматически»)
«Разрешить переопределение значений через переменные окружения»	Управление переопределением значений параметров Агента BPM через переменные окружения (см. подраздел **Переменные окружения и другие параметры конфигурирования**)

Параметр	Описание
«mTLS»	Выбор режима mTLS для защищенного подключения и взаимной аутентификации. Пример настройки mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места» приведен в подразделе **Пример конфигурирования mTLS между компонентами «Универсальный диспетчер» и «Агент виртуального рабочего места»** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса». Возможные значения: • «Выключено» (по умолчанию) - сертификаты игнорируются, их проверка не производится. Агент ВРМ использует самоподписанный сертификат, если является «Сервером». В этом режиме mTLS не используется, заполнять пункты «Сервер» и «Клиент» не требуется; • «Разрешительный режим» - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен или он недействительный, то он не проверяется. Соединение при этом продолжает работать; • «Строгий режим» - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
«Источник сертификатов»	Тип хранилища сертификатов. Возможные значения: • «Файловая система» - сертификаты располагаются локально, в файловой системе; • «Openbao, SecMan (Platform V)» - сертификаты располагаются во внешнем защищенном хранилище сертификатов; • «Хранилище сертификатов Windows» - сертификаты располагаются локально, в хранилище сертификатов ОС Microsoft Windows
Вкладка «Сервер»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ

Параметр	Описание
«Сертификат»	Путь к серверному сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Закрытый ключ»	Путь к серверному закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент BPM автоматически заменяет значение `{{fqdn}}` на FQDN PM. Также допускается ручное указание FQDN PM
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`
«Тип сертификата»	Область хранилища сертификатов ОС Microsoft Windows. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Возможные значения: • «Машина» - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в `HKEY_LOCAL_MACHINE`; • «Пользователь» - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в `HKEY_CURRENT_USER`
«Сертификат»	Выбор серверного сертификата mTLS. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Для выбора сертификата следует нажать экранную кнопку **[Выберите]**, выбрать нужный сертификат в списке и нажать экранную кнопку **[ОК]**. Для просмотра свойств выбранного сертификата следует нажать экранную кнопку **[Просмотр]**

Параметр	Описание
«Использовать как клиентский сертификат»	Серверный сертификат будет использоваться как клиентский. При активации параметра заполнять вкладку «Клиент» не требуется
Вкладка «Клиент»	
«Цепочка ЦС»	Путь к корневому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/ca_chain` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Сертификат»	Путь к клиентскому сертификату mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/certificate` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Закрытый ключ»	Путь к клиентскому закрытому ключу mTLS. Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-pki://pki?common_name={{fqdn}}#example-dot-com/private_key` В параметре поддерживается использование значения `{{fqdn}}`. При обработке пути Агент ВРМ автоматически заменяет значение `{{fqdn}}` на FQDN РМ. Также допускается ручное указание FQDN РМ
«Пароль»	Пароль к закрытому ключу mTLS (если он защищен паролем). Параметр может быть расположен в защищенном хранилище секретов, в этом случае указывается путь к нему: `hvac-kv://secret#agent/passphrase`

Параметр	Описание
«Тип сертификата»	Область хранилища сертификатов ОС Microsoft Windows. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Возможные значения: • «Машина» - хранилище сертификатов, доступных всем пользователям ОС. Находится в системном реестре в HKEY_LOCAL_MACHINE; • «Пользователь» - хранилище сертификатов, доступных текущему пользователю ОС. Находится в системном реестре в HKEY_CURRENT_USER
«Сертификат»	Выбор клиентского сертификата mTLS. Параметр доступен при выборе значения «Хранилище сертификатов Windows» в параметре «Источник сертификатов». Для выбора сертификата следует нажать экранную кнопку **[Выберите]**, выбрать нужный сертификат в списке и нажать экранную кнопку **[ОК]**. Для просмотра свойств выбранного сертификата следует нажать экранную кнопку **[Просмотр]**

Существующие ограничения:

- не поддерживается работа с отозванными сертификатами и цепочкой сертификатов промежуточных УЦ;
- срок действия сертификатов проверяется только при установлении соединения.



Сертификаты, использующиеся для mTLS должны содержать расширения «authClient» и (или) «authServer». В противном случае их нельзя будет добавить.

При использовании mTLS конфигурационный файл веб-сервера Apache компонента «Универсальный диспетчер» должен быть скорректирован (см. подраздел **Конфигурирование веб-сервера Apache для mTLS** документа СЛЕТ.10001-01 90 01 «Руководство администратора. Настройка программного комплекса»).

После задания значений следует:

- проверить корректность введенных значений, нажав экранную кнопку **[Проверить]**. Результатом проверки должно являться сообщение «Проверка успешно завершена»;
- сохранить значения, нажав на экранную кнопку **[Сохранить]**, а затем закрыть окно при помощи экранной кнопки **[Закрыть]**.



Агент BPM автоматически запускается при загрузке ОС Microsoft Windows и создает правило подключения к BPM для межсетевого экрана. Для ручной настройки правил подключений межсетевого экрана с помощью Агента BPM следует обратиться к подразделу **Настройка для ОС Microsoft Windows**.

Пользователь, подключающийся по протоколу RDP к BPM, автоматически будет добавлен в группу «Пользователи удаленного рабочего стола»

Агентом BPM.

Управление правилами межсетевого экрана ОС Microsoft Windows

Агент BPM предоставляет возможность управления правилами межсетевого экрана гостевой ОС Microsoft Windows, используя интерфейс командной строки (CLI).

Управление правилами межсетевого экрана ОС Microsoft Windows выполняется при помощи команды:

```
> TermideskAgentConfig advfirewall
```

Перечень параметров и аргументов CLI, используемых Агентом BPM, указан в таблице (см. таблицу Параметры управления правилами межсетевого экрана Агента BPM).

Для просмотра созданных или удаленных правил межсетевого экрана можно воспользоваться утилитой «Монитор брандмауэра Защитника Windows».

Таблица 13. Параметры управления правилами межсетевого экрана Агента BPM

Параметр командной строки	Аргумент командной строки	Описание
`--help`	`Не задан`	Вывод справки по использованию параметров командной строки. Для вызова справки нужно выполнить: `TermideskAgentConfig advfirewall --help`
`list`	`Не задан`	Вывод списка правил, заданных для межсетевого экрана. Пример: `TermideskAgentConfig advfirewall list` По умолчанию отображаются поля «name», «port», «status»
	`--fields`	Указание полей, отображаемых при формировании списка правил, заданных для межсетевого экрана. Пример: `TermideskAgentConfig advfirewall list --fields name,status` где: `name` - название правила; `status` - статус правила
	`--to-csv`	Вывод списка правил в формате CSV. Пример: `TermideskAgentConfig advfirewall list --to-csv`

Параметр командной строки	Аргумент командной строки	Описание

`create`	`--port`
	
	`--name`
	
	`--remote-address`
		Создание правила для межсетевого экрана.
		
		Пример:
		
		`TermideskAgentConfig advfirewall create --name RULE --remote-address 198.51.100.15`
		
		где:
		
		`name` - название правила;
		
		`remote-address` - IP-адрес, для которого применяется разрешение

`delete`	`--port`
	
	`--name`
		Удаление правила для межсетевого экрана. При наличии нескольких правил с одинаковым названием, будет удалено только первое правило в списке.
		
		Пример:
		
		`TermideskAgentConfig advfirewall delete --name RULE --port 4005`
		
		где:
		
		`name` - название правила;
		
		`port` - порт, для которого применяется разрешение

`status`	`--port`
	
	`--name`
		Просмотр статуса правила для межсетевого экрана.
		
		Пример:
		
		`TermideskAgentConfig advfirewall status --name RULE`
		
		где:
		
		`name` - название правила

`enable`	`--port`
	
	`--name`
		Активация правила для межсетевого экрана.
		
		Пример:
		
		`TermideskAgentConfig advfirewall enable --name RULE`
		
		где:
		
		`name` - название правила

Параметр командной строки	Аргумент командной строки	Описание

`disable`	`--port`
	
	`--name`
		Деактивация правила для межсетевого экрана.
		
		Пример:
		
		`TermideskAgentConfig advfirewall disable --name RULE`
		
		где:
		
		`name` - название правила

Хранение сертификатов в хранилище Microsoft Windows

Для добавления сертификатов в хранилище Microsoft Windows нужно:

- выбрать нужный файл в формате `.pfx`, нажать правой кнопкой мыши и в контекстном меню выбрать действие «Установить PFX» (см. рисунок Добавление сертификата);

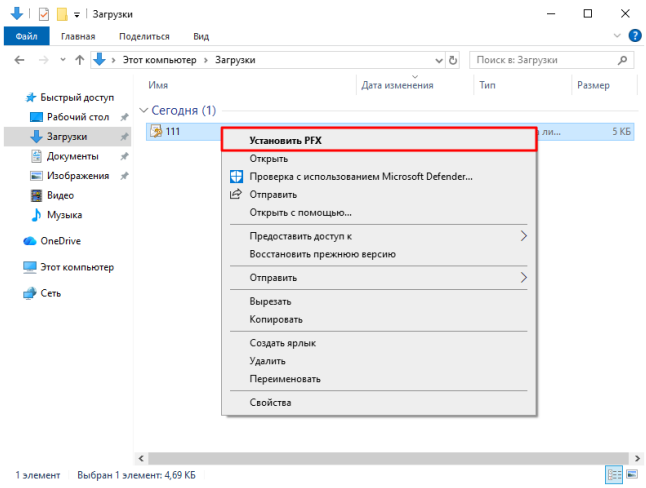


Рисунок 11. Добавление сертификата

- в окне «Мастер импорта сертификатов» указать область хранилища сертификатов и нажать экранную кнопку **[Далее]** (см. рисунок Выбор области хранения сертификатов);

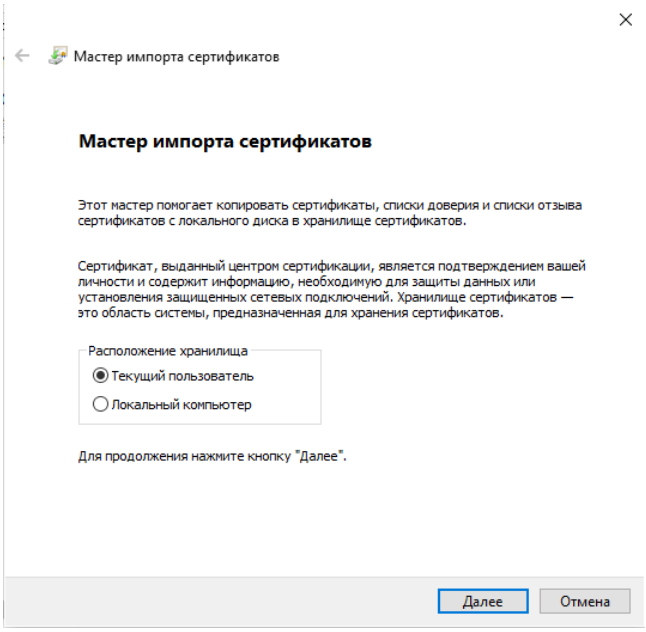


Рисунок 12. Выбор области хранения сертификатов

- в форме «Импортируемый файл» указать путь к файлу в формате `.pfx` (при необходимости) и нажать экранную кнопку **[Далее]** (см. рисунок Указание пути к сертификату);

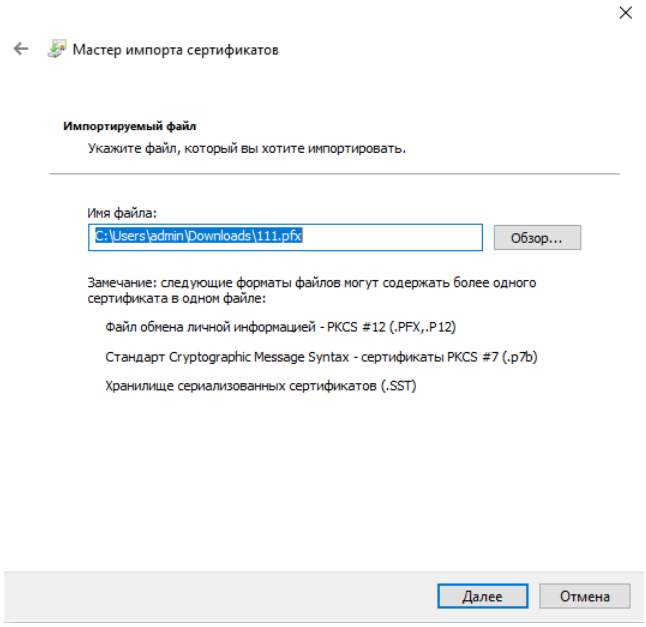


Рисунок 13. Указание пути к сертификату

- в форме «Защита с помощью закрытого ключа» указать пароль, активировать параметр «Пометить этот ключ как экспортируемый, что позволит сохранять резервную копию ключа и перемещать его» и нажать экранную кнопку **[Далее]** (см. рисунок Параметры добавления сертификата);

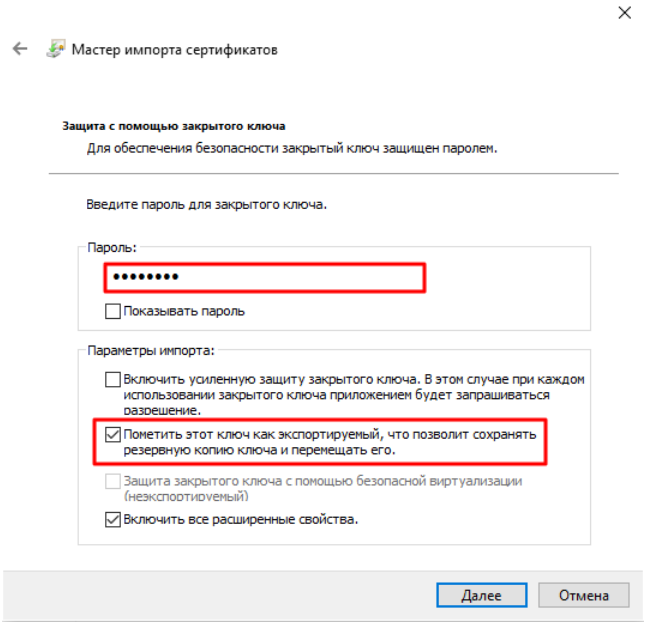


Рисунок 14. Параметры добавления сертификата

- в форме «Хранилище сертификатов» указать хранилище для размещения сертификата, нажать экранную кнопку **[Далее]** (см. рисунок Выбор хранилища сертификатов);

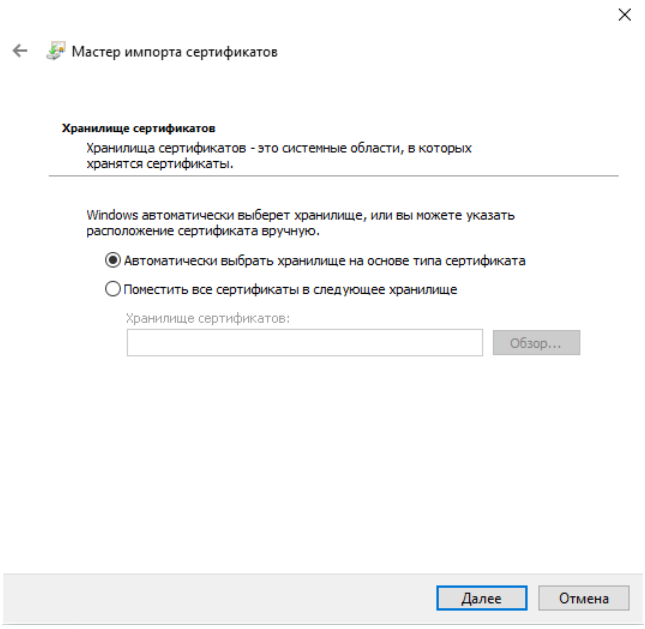


Рисунок 15. Выбор хранилища сертификатов

- ознакомиться с параметрами добавления сертификатов и нажать экранную кнопку **[Готово]**.

Требования к сертификатам:

Параметр «Улучшенный ключ» сертификата должен содержать значения:

- «Проверка подлинности сервера (1.3.6.1.5.5.7.3.1)» - для использования сертификата в качестве серверного;
- «Проверка подлинности клиента (1.3.6.1.5.5.7.3.2)» - для использования сертификата в качестве клиентского.

Допускается наличие обоих значений.

При отсутствии требуемого значения сертификат не отображается в списке доступных сертификатов.

При использовании службы сертификации Active Directory Certificate Services (AD CS) возможность экспорта закрытого ключа должна быть разрешена в свойствах шаблона сертификата и при создании сертификата.

Хранение информации о сессии пользователя

Агент ВРМ поддерживает хранение информации о сессии пользователя, подключившегося к ОС. Этот функционал работает следующим образом:

- пользователь через компонент «Клиент» подключается к серверу Termidesk VDI;
- компонент «Клиент» отправляет серверу (компоненту «Универсальный диспетчер») сведения о пользовательской рабочей станции;
- компонент «Универсальный диспетчер» («Портал пользователя» или «Агрегатор пользователя») получает информацию от компонента «Клиент» и дополняет эти сведения информацией о пользователе и информацией о фонде,и отправляет Агенту ВРМ эти сведения;
- Агент ВРМ сохраняет полученные сведения:
  - для ОС Microsoft Windows: в параметре реестра `HKEY_LOCAL_MACHINE\SOFTWARE\Termidesk\Session\<идентификатор_сессии>`;
  - для ОС Linux: в файле `/var/lib/termidesk/agent/metrics.json`. Файл можно изменить через конфигурационный файл `agent.cfg` в параметре `filepath` (см. подраздел **Конфигурационный файл Агента ВРМ**);
- по API-запросу `/health/metrics` Агент ВРМ вернет полную информацию о сессии пользователя (сведения о пользовательской рабочей станции и метрики сессии).

Сведения о сессии пользователя:

- хранятся для всех сессий, существующих в текущий момент времени;
- создаются при создании сессии и удаляются при ее завершении (logoff);
- доступны для чтения пользователям, но не доступны для изменения.

Перечень параметров, хранимых Агентом ВРМ, приведен в таблице (см. рисунок Перечень параметров, хранимых Агентом ВРМ).

Не все указанные в таблице параметры будут записаны значениями.

Запись актуальных значений производится для параметров:

- `AgentVersion`;
- `ClientAddress`;
- `ClientName`;
- `ClientPlatform`;
- `ClientVersion`;
- `DomainName`;
- `GUSI`;
- `Id`;
- `IdleTime`;
- `LastReconnectReason`;

- LastReconnectTimestamp;
- LogonTimestamp;
- PoolName;
- PublishedName;
- ReconnectionsNumber;
- SessionStatus;
- SessionCreateTimestamp;
- SessionDuration;
- StatusChangedTimestamp;
- Uptime;
- URSI;
- UserName;
- UserSid;
- ViewerVersion.

Если для параметра записано значение, но параметр не отображен в перечне, то в текущей версии Termidesk VDI запись актуального значения для него не производится.

Таблица 14. Перечень параметров, хранимых Агентом ВРМ

Параметр	Описание
AgentVersion	Версия Агента ВРМ
AppliedPolicies	Значения политик, полученные от компонента «Универсальный диспетчер» и примененные Агентом ВРМ
ClientAddress	Локальный IP-адрес пользовательской рабочей станции, через который выполнено подключение к ферме Termidesk VDI. Параметр подчиняется настройке «Использовать анонсируемый IP клиента», заданной в «Портале администратора» Termidesk Если у пользовательской рабочей станции существует более одного IP-адреса, то будет записан IP-адрес Агента ВРМ.
ClientName	Полное доменное имя пользовательской рабочей станции
ClientPlatform	Сведения об ОС пользовательской рабочей станции, на которой установлен компонент «Клиент»
ClientVersion	Версия компонента «Клиент»
ColorDepth	Глубина цвета в сессии пользователя
ConnectionMode	Режим подключения (прямой или через шлюз)
DeliveryProtocol	Тип протокола доставки и его название в ферме Termidesk
DisplaysNumber	Количество мониторов в сессии пользователя
DomainName	Имя домена, в котором аутентифицировался пользователь. В случае, если имя домена отсутствует, то записывается имя домена аутентификации Termidesk
GUSI	Текущий глобальный уникальный сессионный идентификатор
Id	Локальный идентификатор сессии пользователя на РМ

Параметр	Описание
IdleTime	Время бездействия пользователя
LastReconnectReason	Причина последнего отключения
LastReconnectTimestamp	Отметка времени последнего переподключения
LogonTimestamp	Отметка времени входа пользователя в РМ
MachineModifiedDate	Дата и время изменения РМ
PoolName	Имя фонда РМ
PublishedName	Имя публикации
ReconnectionsNumber	Количество переподключений в сессию пользователя
ScreenResolution	Разрешение сессии пользователя (экранное)
SessionType	Тип сессии пользователя (рабочий стол или приложение)
SessionStatus	Состояние сессии (active, idle, disconnected)
SessionCreateTimestamp	Отметка времени создания сессии пользователя
SessionDuration	Длительность сессии пользователя
StatusChangedTimestamp	Отметка времени, когда изменилось состояние сессии пользователя
Uptime	Время с момента загрузки
UserName	Имя пользователя, аутентифицировавшегося в Termidesk
UserSid	Security IDentifier (SID) доменного пользователя (записывается для домена MS AD)
URSI	Текущий уникальный идентификатор запуска ресурса в сессии пользователя
ViewerVersion	Версия ПО Termidesk Viewer

Агент виртуальных смарт-карт

Настройка Агента виртуальных смарт-карт

Дополнительная настройка непосредственно Агента смарт-карт обычно не требуется, однако для разрешения нештатных ситуаций может потребоваться включение более подробного уровня журналирования событий драйвера виртуальной смарт-карты:

- уровень журналирования определяется конфигурационным файлом `/etc/reader.conf.d/exconf/vscard`. Этого файла может не быть, в таком случае необходимо создать каталог, перейти в него и создать пустой файл:

```
sudo mkdir -p /etc/reader.conf.d/exconf
cd /etc/reader.conf.d/exconf
sudo touch vscard
```

- для включения отладочного журналирования конфигурационный файл должен содержать единственное значение - `LOGLEVEL` со значением `DEBUG`:

```
LOGLEVEL DEBUG
```

Параметр `LOGLEVEL` определяет уровень журналирования и может принимать значения: `DEBUG`, `INFO`, `ERROR`. При отсутствии файла `/etc/reader.conf.d/exconf/vscard` значение параметра `LOGLEVEL` по умолчанию `INFO`. Это значение может быть переопределено переменной окружения `TDSK_DEBUG`, в таком случае уровень журналирования будет иметь значение `DEBUG`.

Для перенаправления смарт-карт по протоколу TERA нужно выполнить дополнительную настройку:

- удалить файл `/etc/reader.conf.d/type/vscard.spice`:

```
sudo rm /etc/reader.conf.d/type/vscard.spice
```

- скопировать существующий файл на замену удаленного:

```
sudo cp /etc/reader.conf.d/type/vscard.tera /etc/reader.conf.d/type/vscard.spice
```

- перезагрузить службу:

```
sudo systemctl restart pcscd
```

Видеоагент

Настройка видеоагента

Для настройки видеоагента нужно:

- разрешить автоматический запуск после перезагрузки ОС:

```
sudo systemctl enable termidesk-video-agent.servoce
```

- осуществить запуск видеоагента:

```
sudo systemctl start termidesk-video-agent.service
```

Для проверки состояния службы видеоагента ввести команду:

```
sudo systemctl status termidesk-video-agent.service
```

Строка `Active` отображает состояние сервиса, где статус `active (running)` или `active (exited)` свидетельствует об успешном запуске видеоагента и его готовности к работе.

Агент узла виртуализации

Использование альтернативного механизма сброса сессий

Для корректной работы функционала сброса сессий при подключении пользователя по протоколу SPICE к ВРМ, опубликованным на платформе ПК СВ Брест, нужно выполнить настройку:

- на узлах платформы виртуализации добавить пользователя `root` в группы `libvirt` и `libvirt-admin`, и перезапустить службу `opennebula`:

```
sudo usermod -a -G libvirt root
sudo usermod -a -G libvirt-admin root
sudo systemctl restart opennebula
```

- активировать использование альтернативного механизма сброса сессий для Агента УВ, как приведено ниже.

Для использования альтернативного механизма сброса сессий:

- создать исполняемый файл, который должен реализовать механизм сброса сессий, например, `/etc/termidesk/script.sh`. Содержимое исполняемого файла приведено ниже для примера;
- создать каталог `/etc/termidesk/`:

```
sudo mkdir /etc/termidesk
```

- создать файл `script.sh`:

```
sudo nano /etc/termidesk/script.sh
```

- задать исполняемому файлу флаг выполнения:

```
sudo chmod +x /etc/termidesk/script.sh
```

- изменить права на каталог:

```
sudo chmod 755 /etc/termidesk
```

- создать конфигурационный файл `/etc/termidesk/termidesk-vmsd.conf`:

```
sudo nano /etc/termidesk/termidesk-vmsd.conf
```

- изменить права на файл:

```
sudo chmod 644 /etc/termidesk/termidesk-vmsd.conf
```

- установить переменную `LIBVIRT_PASSWORD_SCRIPT`, определив ее в конфигурационном файле `/etc/termidesk/termidesk-vmsd.conf`. Переменная должна содержать путь к исполняемому файлу:

```
LIBVIRT_PASSWORD_SCRIPT=/etc/termidesk/script.sh
```

Пример содержимого исполняемого файла для сброса сессий:

```
#!/bin/sh
#linux-cli$ /path/to/script --protocol=spice --password=no_password
--connected=disconnect sun-123
# где
#--protocol возможные варианты протокола [spice|vnc]
#--password пароль подключения
#--connected действия [ keep | disconnect | fail ]
VM_PROTOCOL=""
VM_PASSWORD=""
VM_CONNECTED=""
VM_ID=""
if [ -z "${1}" ]; then
    echo "Не заданы параметры"
fi

while [ -n "${1}" ]; do
    case "$(echo "${1}" | cut -d'=' -f1)" in
        --protocol)
            VM_PROTOCOL="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        --connected)
            VM_CONNECTED="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        --password)
            VM_PASSWORD="$(echo "${1}" | cut -d'=' -f2)"
            ;;
        *)
            [ "$(echo "${1}" | grep -i "one-")" ] && VM_ID="${1}"
            ;;
    esac
    shift
done

if [ -n "$(echo "$VM_CONNECTED" | grep -i "disconnect")" ]; then
    IP_PORT=$(ps ax| grep -i "guest=${VM_ID}[^0-9]" | grep -v grep | sed -E -e
"s/.*[[:space:]]+\-${VM_PROTOCOL}[[:space:]]+//" | cut -d' ' -f1 | sed "s/port=//"
| cut -d',' -f1)
    echo "VM SPICE port: $IP_PORT"
    if [ "$IP_PORT" ]; then
        ss --kill -t src :${IP_PORT}
```

```
    fi
fi
```

Сессионный Агент

Конфигурационные файлы сессионного Агента

Конфигурационный файл `session_agent.ini`

Для настройки сессионного Агента используется конфигурационный файл:

- для ОС Astra Linux Special Edition (Server) - `/etc/opt/termidesk-session-agent/session_agent.ini`;
- для ОС Microsoft Windows Server - `C:\ProgramData\UVEON\Termidesk Session Agent\session_agent.ini`.

Администратор может изменить каталог хранения на этапе установки или (в ОС Linux) после установки через переменную окружения `CONFIG_DIR`, указанную в файле `/etc/default/termidesk-session-agent`.

Доступные в конфигурационном файле параметры приведены в таблице (см. таблицу Параметры конфигурирования сессионного Агента).

Таблица 15. Параметры конфигурирования сессионного Агента

Параметр	Значение по умолчанию	Описание
Сетевые настройки		
LISTEN_IP	0.0.0.0	IP-адрес или FQDN сессионного Агента
LISTEN_PORT	31000	Порт сессионного Агента
URL_BALANCER	Не задано	Параметр необходимо задать для работы аутентификации по билету Kerberos на терминальных серверах MS RDS. URL-адрес «Универсального диспетчера» с любой из ролей: «Портал администратора», «Портал пользователя», «Портал универсальный». Для распределенной установки Termidesk VDI указывается узел балансировщика, который будет перенаправлять подключение на нужный узел «Универсального диспетчера». Если значение в параметре не задано, то для отправки сообщений будет использоваться IP-адрес «Универсального диспетчера» из БД сессионного Агента, который записывается при автоматической регистрации со стороны «Универсального диспетчера». Для распределенной установки Termidesk VDI следует указывать значение этого параметра в конфигурационном файле. Необходимо учесть, что узел «Универсального диспетчера» должен уметь разрешать FQDN узла сессионного Агента в IP-адрес. Для этого необходимо, чтобы на DNS-сервере были добавлены записи типа «A» и «PTR». Примеры: URL_BALANCER = https://192.168.0.2 URL_BALANCER = https://disp.termidesk.ru URL_BALANCER = http://192.168.0.2
Настройки мониторинга		

Параметр	Значение по умолчанию	Описание
METRICS_ACCESS_KEY	None	Ключ доступа для аутентификации запросов к API /health/metrics. Значение по умолчанию: None (ключ не задан, проверка запроса на аутентификацию не осуществляется). При задании значения ключа следует руководствоваться правилом, что: • размер ключа должен составлять от 0 до 64 символа; • должны использоваться символы в шестнадцатеричной системе (0-9, a-f)
Настройки взаимодействия с сервером терминалов MS RDS		
INSTALL_RDS_ROLE_ON_NEXT_BOOT	False	Управление ролью сервера терминалов в ОС Microsoft Windows Server. Применяется только при использовании поставщика ресурсов Метапоставщик в Termidesk VDI. Возможные значения: • True - активировать роль сервера терминалов. После активации будет добавлено правило для сессионного Агента в межсетевом экране (брандмауэре) Windows; • False - выключить роль сервера терминалов. После запуска сессионного Агента значение параметра вновь изменится на False, поскольку операция активации выполняется единожды
MASTER_KEY	None	Параметр необходимо задать для работы аутентификации по билету Kerberos на терминальных серверах MS RDS. Значение мастер-ключа «Портала администратора», с которым обменивается данными сессионный Агент
Настройки взаимодействия со STAL		
OTP_TOKEN_TTL	30	Время жизни (в секундах) одноразового токена, использующегося для аутентификации компонента «Клиент» в рамках инициализации сессии пользователя на компоненте «Сервер терминалов Astra Linux»
STAL_TOKEN_TTL	30	Время жизни (в секундах) одноразового токена, использующегося для аутентификации пользователя при подключении к компоненту «Сервер терминалов Astra Linux» с использованием смарт-карт

Параметр	Значение по умолчанию	Описание
STAL_CONNECT_RDP_TTL	10	 Если версия компонента «Сервер терминалов Astra Linux»: • соответствует версии 3.0, то требуется изменить значение на 600; • ниже 3.0, то значение по умолчанию (10) можно не менять. Время ожидания (в секундах) подключения к компоненту «Сервер терминалов Astra Linux»

Параметр	Значение по умолчанию	Описание
USE_USER_PRINCIPAL_NAME	Auto	 Если версия компонента «Сервер терминалов Astra Linux»: • соответствует или выше 4.0, то параметр не используется; • соответствует 3.0, то поддерживается значение Auto; • ниже 3.0, то поддерживаются только значения True или False. Параметр управляет подстановкой суффикса домена. Возможные значения: • True - к имени пользователя будет добавлен суффикс домена. Для этого рекомендуется настроить SSSD-сервисы ОС, задав параметру use_fully_qualified_names значение True. Параметр может быть сконфигурирован: ▫ в файле /etc/sssd/sssd.conf. Если параметр переопределен в файлах каталога /etc/sssd/conf.d/, то их обработка будет приоритетной; ▫ в файлах, размещенных в /etc/sssd/conf.d/. Любой файл из каталога, заканчивающийся на .conf и не начинающийся с точки, будет использоваться вместе с /etc/sssd/sssd.conf. Файлы могут иметь приоритет обработки; • False - имя пользователя не будет модифицироваться; • Auto - автоматическое применение действий: ▫ для локальных пользователей суффикс домена не будет подставлен; ▫ для доменных пользователей выполнится запрос к «Серверу терминалов Astra Linux» для проверки свойства use_fully_qualified_names: ▫ если возвращен ответ True (ожидается имя в формате userPrincipalName), то: ▫ при наличии доменной части имя пользователя остается без изменений; ▫ при отсутствии доменной части имя пользователя модифицируется с добавлением суффикса домена; ▫ если возвращен ответ False (ожидается имя в формате sAMAccountName) то: ▫ при наличии доменной части вызывается исключение; ▫ при отсутствии доменной части имя пользователя остается без изменений. Значение по умолчанию: Auto

Параметр	Значение по умолчанию	Описание
DBUS_TIMEOUT	25	Время ожидания (в секундах) выполнения запросов создания сессии в шине DBUS
REMOVE_INACTIVE_SESSION_FREQUENCY	30	Периодичность (в секундах) запуска задачи удаления неактивных сессий
APPS_SHARING_SESSIONS	None	Параметр используется для запуска приложений, использующих профили пользователя. Список многопрофильных приложений, которые должны быть открыты в том же окне ПО Termidesk Viewer. По умолчанию список не задан и приложения открываются в новых окнах ПО Termidesk Viewer. Если приложение из списка повторно запускается пользователем, то новая сессия будет запущена в рамках уже существующей, а уникальный идентификатор запуска ресурса новой сессии перестанет существовать, будет использоваться ранее назначенный. Для перечисления нескольких приложений следует использовать разделитель - запятую. Пример: APPS_SHARING_SESSIONS = chromium,yandexbrowser
Настройки взаимодействия с сервером терминалов Метапоставщика		

Параметр	Значение по умолчанию	Описание
MAX_SESSIONS	181 или 250	 Параметр действует на терминальный сервер, если он используется в поставщике ресурсов Метапоставщик. Если в поставщике ресурсов параметр «Применить "Сессий всего"» не используется, то предел количества подключений будет зависеть от значения параметра MAX_SESSIONS. При этом количество сессий на узле может быть больше указанного в MAX_SESSIONS значения, если в поставщике ресурсов используются параметры «Соиспользование сессий» и «Предпочитать соиспользование сессий вместо балансировки». Максимально допустимое количество сессий на терминальном сервере. Значение параметра отправляется совместно с метриками узла терминального сервера. Возможные значения: • 181 - для терминального сервера компонента «Сервер терминалов Astra Linux»; • 250 - для терминального сервера MS RDS. Значение по умолчанию определяется автоматически, в зависимости от терминального сервера, на который установлен сессионный Агент
Настройки подключения по протоколу HTTPS		
USE_HTTPS	False	Управление запуском сессионного Агента в режиме использования протокола HTTPS. Возможные значения: • True - используется протокол HTTPS, запросы по протоколу HTTP не обрабатываются; • False - используется протокол HTTP. Необходимо настроить «Портал администратора» на использование протокола HTTP, скорректировав файл /etc/apache2/sites-available/termidesk.conf (см. подраздел **Перенаправление на HTTPS** документа СЛЕТ.10001-01 90 02 «Руководство администратора. Настройка программного комплекса»)

Параметр	Значение по умолчанию	Описание
VERIFY_CERT	False	Управление проверкой SSL-сертификата в режиме использования протокола HTTPS. При использовании режима mTLS параметр VERIFY_CERT игнорируется. Возможные значения: • True - проверка SSL-сертификата включена. Режим работы: HTTPS с проверкой сертификата; • False - проверка SSL-сертификата отключена. Режим работы: HTTPS без проверки сертификата, или HTTP (если параметр USE_HTTPS=False). Если используется значение True, то на узел должен быть загружен корневой сертификат: • если путь указан в параметре CA_CERTIFICATE_PATH, то будет использоваться сертификат, указанный в значении этого параметра; • если путь не указан в параметре CA_CERTIFICATE_PATH, то будет использоваться сертификат из системного хранилища сертификатов
CERTIFICATE_PATH	/etc/opt/termidesk-session-agent/certs/cert.pem или C:\ProgramData\UVEON\Termidesk Session Agent\certs\cert.pem	Путь до SSL-сертификата. Для ОС Astra Linux Special Edition: /etc/opt/termidesk-session-agent/certs/cert.pem. Для ОС Microsoft Windows Server: C:\ProgramData\UVEON\Termidesk Session Agent\certs\cert.pem
PRIVATE_KEY_PATH	/etc/opt/termidesk-session-agent/certs/key.pem или C:\ProgramData\UVEON\Termidesk Session Agent\certs\key.pem	Путь до закрытого ключа. Для ОС Astra Linux Special Edition: /etc/opt/termidesk-session-agent/certs/key.pem. Для ОС Microsoft Windows Server: C:\ProgramData\UVEON\Termidesk Session Agent\certs\key.pem
Настройки взаимной аутентификации mTLS		

Параметр	Значение по умолчанию	Описание
MTLS_MODE	0	Режим mTLS для защищенного подключения и взаимной аутентификации. Возможные значения: • 0 - сертификаты игнорируются, их проверка не производится. В этом режиме mTLS не используется; • 1 - нестрогий режим проверки сертификата. Проверка выполняется, но если сертификат не предоставлен, или он недействительный, или возникли ошибки при его проверке, то это не приведет к разрыву соединения; • 2 - строгий режим проверки сертификата. Предоставление действительных сертификатов обязательно. Соединение сбрасывается, если сертификат не прошел проверку
CIPHERS	TLSv1.2	Протокол подключения для mTLS. Возможные значения: • TLSv1.2; • TLSv1.3
CA_CERTIFICATE_PATH	Не задано	Путь к корневому сертификату mTLS
CLIENT_CERTIFICATE_PATH	Не задано	Путь к клиентскому сертификату mTLS
CLIENT_PRIVATE_KEY_PATH	Не задано	Путь к клиентскому закрытому ключу mTLS. Ключ может иметь парольную защиту. Для использования ключа нужно преобразовать его к начальному значению: openssl rsa -in <путь_к_файлу_ключа.key> -out <путь_сохранения_преобразованного_ключа.key>
Настройки журналирования		
LEVEL	INFO	Уровень журналирования. Допустимые значения: NOTSET, DEBUG, INFO, WARNING, ERROR, CRITICAL
ROTATION_LIMIT	5	Максимальное количество файлов журналов. После достижения предела, происходит сжатие журналов в архив
MAX_FILE_SIZE	2097152	Максимальный размер файла журнала (в байтах)

Параметр	Значение по умолчанию	Описание

`LOG_DIR`	`/var/log/termidesk`	Задает каталог хранения журналов сессионного Агента.
		
		Пример: администратор хочет изменить место хранения журналов сессионного Агента.
		
		Для этого администратору нужно:
		
		• создать нужный каталог. Каталог должен обладать свойствами:
		  ◦ права доступа: `rwxr-xr-x` (в восьмеричной записи - `755`);
		  ◦ владелец и группа: `termidesk:termidesk`;
		• задать параметру новое значение;
		• перезапустить службу `termidesk-session-agent`:
		
		`sudo systemctl restart termidesk-session-agent`

`SEND_LOGS_TO_REPEATER`	`False`	Управление отправкой журналов событий на компонент «Ретранслятор». Возможные значения: • `True` - события отправляются на компонент «Ретранслятор»; • `False` - события не отправляются на компонент «Ретранслятор»

Файл /etc/default/termidesk-session-agent

Одним из параметров службы termidesk-session-agent является аргумент EnvironmentFile, задающий путь к дополнительным аргументам запуска, перечисленным в файле /etc/default/termidesk-session-agent.

Файл /etc/default/termidesk-session-agent:

- автоматически создается в ОС при установке сессионного Агента;
- если файл существует, то происходит его построчное чтение в формате <ключ>=<значение> и в запускаемый процесс сессионного Агента добавляются переменные окружения (см. подраздел **Переменные окружения и аргументы командной строки**).

Есть ряд переменных окружения, которые требуются для нормального функционирования сессионного Агента. Такими переменные окружения являются:

Эти переменные окружения запрещено удалять или модифицировать. Переменные, доступные для модификации, перечислены в подразделе **Переменные окружения и аргументы командной строки**.

- SHELL;
- USER_TERMIDESK;
- GROUP_TERMIDESK;
- HOME_DIR;
- VIRTUAL_ENV.

Первичная настройка

В обычной конфигурации настройка сессионного Агента не требуется.

Сертификаты открытого ключа (cert.pem) и закрытый ключ (key.pem), используемые сессионным Агентом для формирования токенов и взаимодействия с другими компонентами Termidesk VDI, генерируются автоматически.

Сертификаты и ключ расположены в каталоге:

- для ОС Astra Linux Special Edition (Server) и ОС Альт Рабочая станция - /etc/opt/termidesk-session-agent/certs/;
- для ОС Microsoft Windows Server - C:\ProgramData\UVEON\Termidesk Session Agent\certs\.

Настройка сессионного Агента на использование протокола HTTPS

По умолчанию после установки сессионный Агент использует протокол HTTP для обработки запросов. Для того чтобы сессионный Агент обрабатывал запросы по протоколу HTTPS нужно:

- выполнить импорт сертификата и ключей на узел с сессионным Агентом;
- указать пути к сертификату и ключу в параметрах конфигурации сессионного Агента session_agent.ini;
- присвоить параметру USE_HTTPS значение True в параметрах конфигурации сессионного Агента session_agent.ini;
- выполнить перезапуск службы «TermideskSessionAgentService» через оснастку «Службы» в ОС Microsoft Windows Server или командой в ОС Astra Linux Special Edition

(Server):

```
sudo systemctl restart termidesk-session-agent
```

После выполненных действий необходимо включить параметр «Использовать HTTPS» в настройках поставщика «Сервер терминалов» в веб-интерфейсе Termidesk VDI.

Активация роли терминального сервера в ОС Microsoft Windows Server

Этот подраздел настроек используется только при использовании поставщика ресурсов Метапоставщик в Termidesk VDI.

Для тиражирования приложений ОС Microsoft Windows Server необходимо после установки роли «Remote Desktop Session Host» из состава «Remote Desktop Services» выполнить активацию через сессионный Агент. Для этого нужно присвоить параметру `INSTALL_RDS_ROLE_ON_NEXT_BOOT` значение `True` в параметрах конфигурации сессионного Агента `session_agent.ini`.

АГЕНТ. ЖУРНАЛИРОВАНИЕ

Журналы работы Агентов

Журналы работы Агента ВРМ расположены в следующих файлах:

- ОС Linux:
  - журналы непосредственно Агента ВРМ: для непривилегированного пользователя `~/.config/UVEON/logs/termidesk_agent.log`, для службы `/var/log/termidesk/agent.log`;
  - журнал драйвера печати CUPS: `/var/log/termidesk/cups_daemon.log`;
- ОС Microsoft Windows:
  - для непривилегированного пользователя `%APPDATA%\UVEON\logs\termidesk_agent.log`;
  - для службы `%PROGRAMDATA%\UVEON\logs\termidesk_agent.log`.

Каталог хранения журналов Агента ВРМ в ОС Linux может быть переопределен через конфигурационный файл `/etc/termidesk/agent.cfg` или переменные окружения `TDSK_LOG_SRV_DIR` и `TDSK_LOG_USER_DIR`.

Агент ВРМ поддерживает ротацию журналов работы `agent.log` и `termidesk_agent.log`. Настройка ротации выполняется через переменные окружения `TDSK_LOG_ROTATE_MAX_SIZE` и `TDSK_LOG_ROTATE_MAX_SIZE`.

Журнал Агента ВРМ можно также просмотреть в системном журнале ОС Microsoft Windows. Для этого (см. рисунок Расположение событий Агента в системном журнале ОС Microsoft Windows):

- перейти «Пуск - Средства администрирования Windows - Просмотр событий»;
- в открывшемся окне перейти по дереву «Журналы Windows - Приложение»;
- затем в доступных действиях выбрать «Фильтр текущего журнала» и задать в поле «Источники событий» значение «Termidesk Agent»;
- нажать экранную кнопку **[OK]**.

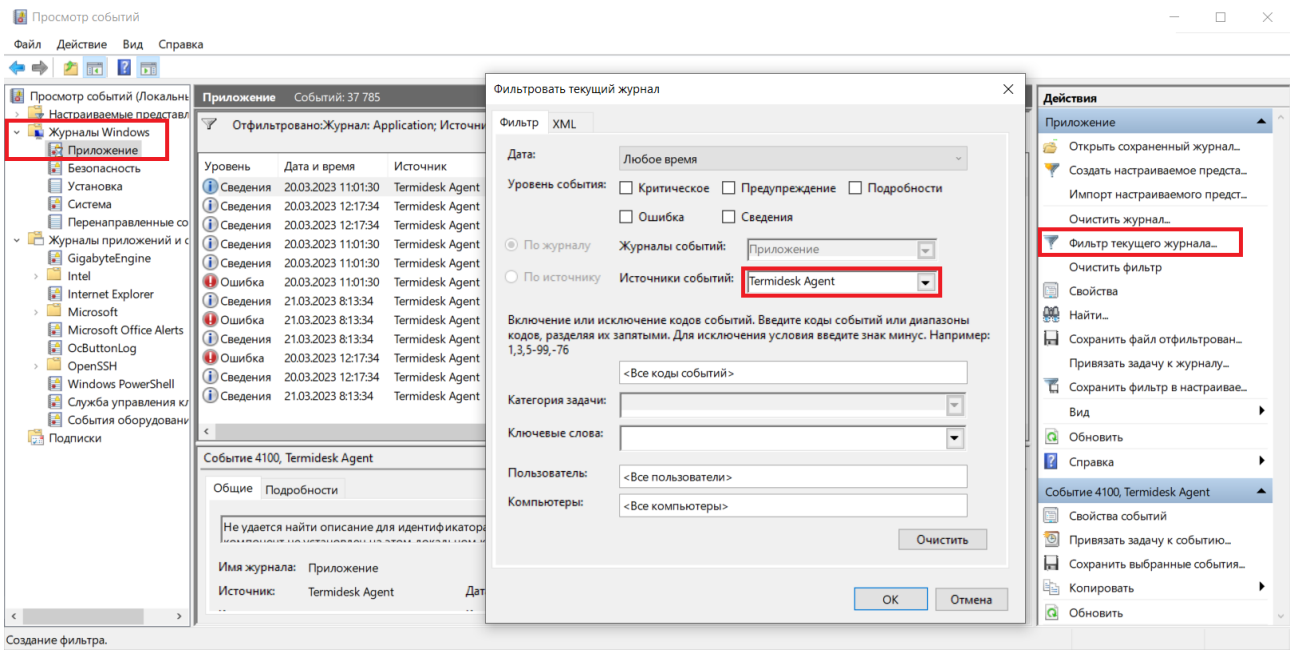


Рисунок 16. Расположение событий Агента в системном журнале ОС Microsoft Windows

Журналы работы сессионного Агента расположены в следующих файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/session-agent.log`;
- ОС Microsoft Windows: `%PROGRAMDATA%\UVEON\Termidesk Session Agent\log\session-agent.log`.



Администратор может изменить каталог хранения на этапе установки или (в ОС Linux) после установки через параметр `LOG_DIR`, указанный в конфигурационном файле `/etc/opt/termidesk-session-agent/session_agent.ini`.

События создания файла БД, очистки БД и записи метрик в нее регистрируются в журнале сессионного Агента.

Журналы работы Агента виртуальных смарт-карт расположены в следующих файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/pcscd.log`.

События, связанные с видеоагентом, регистрируются в журнале `syslog` (сообщения о статусе запуска службы), а также файлах:

- ОС Astra Linux Special Edition: `/var/log/termidesk/video_agent.log`;
- ОС Microsoft Windows: `%PROGRAMDATA%\UVEON\logs\termidesk_video_agent.log`.

Для просмотра событий, регистрируемых в журнале `syslog`, можно воспользоваться инструментом `journalctl` и отсортировать вывод событий по тексту «video» утилитой `grep`. Пример:

```
sudo journalctl | grep 'video'
```

Журнал работы Агента УВ расположен в файле `/var/log/termidesk/agent.log`.

В журналах регистрируются следующие события:

- информация о запуске Агента;
- информация о настройке Агента;
- сообщения, передаваемые между Агентом и компонентом «Универсальный диспетчер»;
- сообщения, передаваемые от администратора к пользователю ВРМ;
- время простоя ВРМ;
- подключение и отключение пользователя к ВРМ по протоколу RDP;
- подключение переносимых профилей (при включении соответствующего функционала);
- в журналах сессионного Агента и Агента ВРМ регистрируется информация о глобальном уникальном идентификаторе сессии, позволяющим однозначно сопоставить пользователя и производимые им действия;
- в журналах сессионного Агента и Агента ВРМ также регистрируется информация об уникальном идентификаторе запуска ресурса, позволяющим однозначно сопоставить пользователя и доступные ему ресурсы: ВРМ и приложения.

Сбор и передача событий аутентификации, блокировки и разблокировки сессии

Агент ВРМ поддерживает мониторинг и запись событий аутентификации, блокировки и разблокировки пользовательской сессии в гостевой ОС, и их передачу в журнал РМ «Портала администратора».

Функционал сбора событий для разных ОС отличается:

- ОС Microsoft Windows: производится подписка на события. То есть, ОС Microsoft Windows присылает события в сторону Агента ВРМ, который их разбирает и отправляет в журнал РМ;
- ОС Linux: производится мониторинг событий журнала аудита ОС Linux Агентом ВРМ.

Для событий фиксируются:

- `elapsed` - время (в секундах) с момента отправки запроса параметров подключения от ПО Termidesk Viewer и до авторизации в гостевой ОС (API-запрос `/preConnect`);
- `user` - имя пользователя РМ;
- результат действия, например: `UNLOCK SUCCESS` (успешная разблокировка), `Auth SUCCESS` (успешная аутентификация);
- `logon_id` - (для ОС Microsoft Windows) уникальный идентификатор пользовательской сессии в ОС (создается непосредственно ОС). Используется для сопоставления пользовательской сессии и отслеживания ее жизненного цикла;
- `logon_type` - (для ОС Microsoft Windows) тип авторизации пользователя. Возможные коды и их описания приведены в таблице (см. таблицу Возможные коды для параметра `logon_type`). Описание от производителя ОС Microsoft Windows приведено по ссылке: https://learn.microsoft.com/ru-ru/windows-server/identity/securing-privileged-access/reference-tools-logon-types;
- `auth_type` - тип аутентификации пользователя. Возможные значения и их описания приведены в таблице (см. таблицу Возможные значения для параметра `auth_type`);
- `reason` - (для ОС Microsoft Windows) причина ошибки. Возможные коды и их описания приведены в таблице (см. таблицу Возможные коды для параметра `reason`);
- `session_id` - (для ОС Linux) уникальный идентификатор пользовательской сессии в ОС.

Примеры записи событий:

- ОС Microsoft Windows, первая авторизация (RDP):

```
Security events monitoring. Auth SUCCESS | session_id=0x690183 user=cld@test-
win1000000 logon_type=10 auth_type=negotiate total=1
Security events monitoring. Auth SUCCESS | session_id=0x685f78 user=cld@test-
win1000000 logon_type=3 auth_type=plain total=1 elapsed=5.703s
```

- ОС Microsoft Windows, разблокировка сессии (RDP):

```
Security events monitoring. Workstation UNLOCK SUCCESS | logon_id=0x77ef2d
user=cld@test-win1000000 auth_type=negotiate total=1
Security events monitoring. Workstation UNLOCK FAILURE | logon_id=0x3e7
user=cld@test-win1000000 auth_type=negotiate reason=%%2313 total=2
```

- ОС Linux, первая авторизация:

```
Security events monitoring. Auth SUCCESS | user=admin123 auth_type=plain
total_success=1 elapsed=11.169s
```

- ОС Linux, блокировка и разблокировка сессии:

```
Security events monitoring. Workstation UNLOCK | user=admin123
Security events monitoring. Auth FAILURE | user=admin123 auth_type=plain
total_failure=1
Security events monitoring. Workstation LOCK | user=admin123 cause=user
```

Таблица 16. Возможные коды для параметра `logon_type`

Код	Название	Описание
`0`	System	Системный вход
`2`	Interactive	Локальный вход
`3`	Network	Сетевой доступ
`4`	Batch	Планировщик задач
`5`	Service	Сервис
`7`	Unlock	Разблокировка
`8`	NetworkCleartext	Пароль в явном виде
`9`	NewCredentials	Сетевой доступ, но с сохранением локальной сессии
`10`	RemoteInteractive	Удаленный вход по RDP
`11`	CachedInteractive	Кешированный вход
`12`	CachedRemoteInteractive	Удаленный вход по RDP с кешированием
`13`	CachedUnlock	Разблокировка с кешированием

Таблица 17. Возможные значения для параметра `auth_type`

Значение	Описание
`plain`	Простая парольная аутентификация
`kerberos`	Kerberos-аутентификация
`smartcard`	Kerberos-аутентификация по сертификату, размещенному на смарт-карте
`negotiate`	Автоматический выбор наиболее безопасного типа аутентификации: Kerberos или NTLM. Предпочтительно выбирается Kerberos-аутентификация, при необходимости происходит переключение на NTLM. Только для ОС Microsoft Windows
`digest`	Deigest-аутентификация. Только для ОС Microsoft Windows
`schannel`	Аутентификация с использованием протокола SSL/TLS для шифрования сообщений между аутентифицированными сторонами. Только для ОС Microsoft Windows
`cloudap`	Аутентификация Azure AD. Только для ОС Microsoft Windows

Таблица 18. Возможные коды для параметра `reason`

Код	Нормализованное имя	Описание
`%%2304`	account_locked	Учетная запись заблокирована
`%%2305`	account_disabled	Учетная запись отключена
`%%2307`	account_expired	У учетной записи истек срок действия
`%%2309`	invalid_logon_hours	Вход запрещен по времени
`%%2310`	invalid_workstation	Вход запрещен с данного узла
`%%2311`	password_expired	У пароля истек срок действия

Код	Нормализованное имя	Описание
%%2312	account_restriction	Учетная запись ограничена
%%2313	bad_credentials	Неверное имя пользователя или пароль

АГЕНТ. НЕШТАТНЫЕ СИТУАЦИИ И СПОСОБЫ ИХ УСТРАНЕНИЯ

Возможные неисправности при работе с Удаленным помощником и способы их устранения приведены в таблице (см. таблицу Перечень возможных нештатных ситуация и способов их устранения).

Таблица 19. Перечень возможных нештатных ситуация и способов их устранения

Индикация	Описание	Возможное решение

Ошибки авторизации пользователя при подключении к гостевой ОС РМ	Пользователь не может авторизоваться в гостевой ОС при подключении к РМ	Чаще всего ситуация возникает при неправильной настройке модуля pam_tdsk. Для отладки и поиска ошибок в модуле pam_tdsk нужно:
		• создать пользователя с UID < 1000 и GID < 1000 и авторизоваться им в ОС;
		• изменить файл /etc/pam.d/common-session в строке с pam_exec.so:
		`session required pam_exec.so log=/var/log/termidesk/pam_tdsk.log /usr/bin/pam_tdsk.sh`
		• создать дополнительный отладочный файл журнала:
		`touch /var/log/termidesk/pam_tdsk.log`
		• создать исполняемый файл /usr/bin/pam_tdsk.sh, вызывающий pam_tdsk:
		`#!/bin/sh -x`
		`env`
		`SELF_BIN=$(realpath ${0})`
		`SELF_DIR=$(dirname ${SELF_BIN})`
		`args="$@"`
		`pam_tdsk $@`
		`exit_code=$?`
		`exit ${exit_code}`
		• одновременно открыть созданный отладочный файл журнала (/var/log/termidesk/pam_tdsk.log) и стандартный журнал (/var/log/termidesk/agent.log):
		`tail -f /var/log/termidesk/pam_tdsk.log /var/log/termidesk/agent.log`
		• повторить попытку подключения пользователем (допускается как подключение из компонента «Клиент», так и через удаленное подключение по протоколу SSH). Проанализировать сообщения, начинающиеся с pam_tdsk. При необходимости обратиться в техническую поддержку с предоставлением файлов журналов

ТЕРМИНЫ

Компонент «Агент»

Самостоятельный компонент, отвечающий за контролируемую доставку РМ, взаимодействие с «Универсальным диспетчером» и «Менеджером рабочих мест». Собирательное название для следующих компонентов Termidesk VDI:

- «Агент виртуального рабочего места»;
- «Агент узла виртуализации»;
- «Сессионный агент»;
- «Видеоагент»;
- «Агент виртуальных смарт-карт»

Компонент «Агент виртуальных смарт-карт»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление подключенных к пользовательской рабочей станции смарт-карт в ВРМ

Компонент «Агент виртуального рабочего места»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет взаимодействие с «Универсальным диспетчером», конфигурирует ВРМ, фиксирует действия пользователя, реализует передачу управляющих сообщений

Компонент «Агент узла виртуализации»

Компонент Termidesk VDI. Устанавливается на узел виртуализации, взаимодействует с гипервизором через модуль `libvirt`

Базовое виртуальное рабочее место

Также: золотой образ, базовый образ. Подразумевает собой образ диска ВМ с предустановленным прикладным ПО и установленным «Агентом виртуального рабочего места». Этот образ далее будет использоваться для создания ВРМ для пользователей

Компонент «Видеоагент»

Компонент Termidesk VDI. Устанавливается в гостевую ОС при подготовке базового ВРМ. Выполняет перенаправление видеокамеры с пользовательской рабочей станции в ВРМ

Виртуальное рабочее место

Развернутая на ВМ ОС с установленным «Агентом виртуального рабочего места» и необходимым прикладным ПО. Подключение к ВРМ происходит через протоколы удаленного доступа

Рабочее место

Гостевая ОС или ОС, установленная на выделенном компьютере, доступ к которой реализуется с помощью протокола удаленного доступа. Под РМ подразумеваются как ВРМ, так и терминальный доступ или доступ к опубликованным на терминальном сервере приложениям

Гостевая ОС

ОС, функционирующая на ВМ

Компонент «Менеджер рабочих мест»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за взаимодействие с поставщиком ресурсов и управления жизненным циклом РМ, включая создание, настройку, запуск, отключение и удаление. Является обработчиком фоновых задач. Устанавливается из пакета `termidesk-vdi`. Наименование служб после установки: `termidesk-celery-beat.service` и `termidesk-celery-worker.service`

Поставщик ресурсов

ОС, платформа виртуализации или терминальный сервер (MS RDS/STAL), предоставляющие вычислительные мощности, ресурсы хранения данных, а также сетевые ресурсы для размещения фондов РМ

Протокол доставки

Поддерживаемый в Termidesk VDI протокол удаленного доступа к РМ

Компонент «Сессионный агент»

Компонент Termidesk VDI. Устанавливается на терминальный сервер (MS RDS/STAL), активирует возможность множественного доступа пользователей к удаленным рабочим столам и приложениям

Компонент «Универсальный диспетчер»

Компонент Termidesk VDI. Отделяемый компонент программного комплекса, отвечающий за идентификацию пользователей, назначение им РМ и контроля доставки РМ. Устанавливается из пакета `termidesk-vdi`. Наименование службы после установки: `termidesk-vdi.service `

Фонд рабочих мест

Совокупность подготовленных РМ для доставки по одному или нескольким протоколам удаленного доступа в зависимости от полномочий пользователей

Шаблон рабочего места

Параметры конфигурации рабочего места для использования в фонде РМ

Компонент «Сервер терминалов Astra Linux»

Компонент Termidesk VDI. Также: STAL. Обеспечивает подключение пользовательских рабочих станций к РМ с ОС Astra Linux Special Edition через сеанс удаленного терминала

Ключ

Применяется в контексте файла, не опции в команде. Последовательность псевдослучайных чисел, сгенерированная особым образом

Сертификат

Артефакт, содержащий информацию о владельце ключа и подтверждающий принадлежность ключа владельцу

СОКРАЩЕНИЯ

БД	База данных
ВМ	Виртуальная машина
ВРМ	Виртуальное рабочее место
ЗПС	Замкнутая программная среда
ОС	Операционная система
ПК СВ Брест	Программный комплекс «Средства виртуализации «Брест»
ПО	Программное обеспечение
РМ	Рабочее место
УВ	Узел виртуализации
ЦС	Центр сертификации
ЭЦП	Электронная цифровая подпись
API	Application Programming Interface (интерфейс прикладного программирования)
CLI	Command Line Interface (интерфейс командной строки)
CUPS	Common UNIX Printing System (система печати Unix)
DBus	Desktop Bus (система межпроцессного взаимодействия)
DNS	Domain Name System (система доменных имен)
EULA	End-User License Agreement (лицензионное соглашение с конечным пользователем)
FQDN	Fully Qualified Domain Name (полностью определенное имя домена)
HTTP	HyperText Transfer Protocol (протокол передачи гипертекста)
HTTPS	Hypertext Transfer Protocol Secure (расширение протокола HTTP для поддержки шифрования)
IP	Internet Protocol (межсетевой протокол)
MS AD	Microsoft Active Directory Domain Service (службы каталогов Microsoft)
mTLS	Multiplexed Transport Layer Security (протокол, основанный на TLS с усиленной безопасностью)
PCSC	Personal Computer Smart Card (стандарт для взаимодействия между персональными компьютерами и смарт-картами)
RDP	Remote Desktop Protocol (протокол удаленного рабочего стола)
RDS	Remote Desktop Services (службы удаленного рабочего стола)
REST	Representational State Transfer (программная архитектура, определяющая условия работы API)

RFC	Request for Comments (рабочее предложение Интернет)
RPC	Remote Procedure Call (удаленный вызов процедур)
SID	Security IDentifier (уникальный идентификатор безопасности)
SPICE	Simple Protocol for Independent Computing Environments (открытый протокол для удаленного доступа к рабочим столам ВМ)
SSL	Secure Sockets Layer (криптографический протокол)
SSSD	System Security Services Daemon (системная служба, управляющая доступом к удаленным каталогам и механизмам аутентификации)
STAL	Terminal Server Astra Linux (компонент «Сервер терминалов Astra Linux»)
TERA	Termidesk Remote Access protocol (протокол удаленного доступа разработкиООО «УВЕОН»)
UAC	User Account Control User (контроль учетных записей пользователей)
URL	Uniform Resource Locator (унифицированный указатель ресурса)
USB	Universal Serial Bus (последовательный интерфейс для подключения периферийных устройств)

UVEON



© ООО «Увеон»

Телефон: +7 495 975 19 75
8 800 222 07 00

Электронная почта для связи: info@uveon.ru

Отдел продаж: info@astralinux.ru
Техподдержка: termidesk@astralinux.ru

Сайт: https://termidesk.ru/

Главный офис 119571, г. Москва,
Ленинский проспект, д. 119А