TERMIT

Termit Apps Advanced

Руководство администратора

WIKI.ORIONSOFT.RU

Содержание

1. Вход в систему . . . 5
2. Обзор . . . 7
   Группы доставки . . . 7
   Компоненты . . . 10
   Пиковая активность . . . 11
   Пользователи . . . 11
   Приложения . . . 12
   Ошибки . . . 13
   Время входа . . . 13
   Динамика сессий . . . 14
3. Журнал событий . . . 16
   Список событий . . . 16
   Экспорт данных в CSV . . . 25
4. Каталоги ресурсов . . . 26
   Виды каталогов ресурсов . . . 26
   Статусы и действия с каталогом ресурсов и серверами . . . 26
   Просмотр информации о каталоге ресурсов . . . 26
   4.1. Статусы и действия с каталогом ресурсов и серверами . . . 27
      Перевод ТС на обслуживание . . . 27
      Снятие ТС с обслуживания . . . 28
      Работа с агентом . . . 28
      Удаление сервера из каталога ресурсов . . . 30
      Удаление каталога ресурсов . . . 30
   4.2. Терминальные серверы . . . 31
      Создание каталога ресурсов . . . 31
      Изменение настроек терминальных серверов . . . 32
5. Группы доставки . . . 34
   Просмотр информации о группе доставки . . . 34
   Создание группы доставки . . . 35
   Подключение сетевых дисков . . . 36
   Изменение группы доставки . . . 37
   Перевод группы доставки в режим обслуживания . . . 38
   Вывод группы доставки из режима обслуживания . . . 38
   Отсоединение пользователя от сервера . . . 39
   Управление задачами . . . 39
   Удаление группы доставки без зависимостей . . . 41

Удаление группы доставки с зависимостями . . . 41
6. Приложения . . . 43
Добавление приложения . . . 43
Просмотр информации о приложении . . . 46
Изменение параметров приложения . . . 46
Выключение приложения . . . 48
Включение приложения . . . 48
Удаление приложения . . . 48
Скачивание файла подключения к ТС . . . 48
Экспорт данных в CSV . . . 49
Ограничение запуска нескольких экземпляров приложений . . . 49
7. Сессии . . . 51
Статусы сессий . . . 51
Подключение в сессию сотрудника . . . 51
Завершение сессии . . . 52
Экспорт данных в CSV . . . 52
8. Политики . . . 53
8.1. Общие . . . 53
Статусы политик . . . 53
Описание настроек политик . . . 53
Описание вкладки «Общие» . . . 56
Создание политики . . . 56
Балансировка терминальных сессий . . . 59
Включение политики . . . 61
Выключение политики . . . 61
Перевод политики в статус «Моделирование» . . . 61
Изменение приоритета политики . . . 62
Изменение политики . . . 63
Удаление политики . . . 64
8.2. Моделирование . . . 65
Создание моделирования . . . 66
Проведение повторного моделирования . . . 67
Просмотр отчета о моделировании . . . 67
Удаление моделирования . . . 67
9. Настройки . . . 68
9.1. Общие настройки . . . 68
HTTPS . . . 68
Внешний вид десктоп-клиента . . . 68

Аутентификация 69
Многофакторная аутентификация 69
Пользовательский портал 70
Syslog/SIEM 71
Доверенные сертификаты 71
Администратор системы 72
Глубина хранения журналов событий 73
Глубина хранения сессий 74
RADIUS 74
Политика блокировки встроенных учетных записей 76
Токены 77
9.2. LDAP-каталоги 78
Добавление LDAP-каталога 79
Изменение настроек LDAP-каталога 84
Удаление LDAP-каталога 88
Настройка Kerberos 89
9.2.1. Настройка Kerberos 89
9.3. Категории 97
Создание новой категории 97
Изменение настроек категории 98
Удаление категории 98
9.4. Внешний доступ 99
Настройка внешнего подключения 100
Добавление шлюза 101
Перевод шлюза в режим обслуживания 101
Перевод шлюза из режима обслуживания 102
Удаление шлюза 102
9.5. Зоны 102
Добавление зоны 102
Редактирование зоны 103
Удаление зоны 103
10. Брокеры 104
Удаление брокера 104
Экспорт данных в CSV 104
11. Пользователи 106
Просмотр информации о пользователе 106
Блокировка пользователя 106
Разблокировка пользователя 107

Закрытие сессий пользователя . . . 107
Экспорт данных в CSV . . . 108
12. Права доступа . . . 109
12.1. Назначения . . . 109
Создание назначения . . . 109
Клонирование назначения . . . 110
Изменение назначения . . . 110
Удаление назначения . . . 111
12.2. Роли . . . 111
Создание роли . . . 112
Клонирование роли . . . 112
Изменение роли . . . 113
Удаление роли . . . 113
12.3. Области видимости . . . 114
Создание области видимости . . . 114
Клонирование области видимости . . . 115
Изменение области видимости . . . 116
Удаление область видимости . . . 116
12.4. Выражения SpEL в областях видимости . . . 117
Задание выражения . . . 117
Принцип работы . . . 117
Свойства объектов . . . 118
Примеры . . . 121
Рекомендации . . . 121
13. Профили пользователей . . . 122
13.1. Настройка профиля пользователя в терминальной среде Windows . . . 122

Глава 1. Вход в систему

Чтобы войти на портал администрирования Termit:

1. В адресной строке браузера введите адрес портала внутреннего/внешнего доступа.
2. На главной странице:
   a. Выберите домен:

Домен — это система, которая определяет права доступа пользователей (т.е., что им разрешено делать после входа). Например, это может быть Active Directory или встроенная база данных.

- **Авто**. Система автоматически выберет LDAP-каталог из списка доступных каталогов или внутренних пользователей.
- **Внутренние пользователи**. Вход будет выполнен под учетной записью локального администратора «tadm».
- **Имя LDAP-каталога**, отображаемое полное имя которого было задано при добавлении в систему, например «ldap123».

   b. Для входа под учетной записью администратора системы укажите в поле ввода:
   - **Логин** — введите логин.
   - **Пароль** — введите пароль.
   - **Одноразовый код** — введите полученный из приложения-аутентификатора одноразовый пароль.

1. Для входа под учетной записью локального администратора используйте по умолчанию логин `tadm` и пароль `admin`.
2. Локальная учетная запись предназначена только для настройки брокера. Ее нельзя использовать для входа в десктоп-клиент, запуска приложений и рабочих столов.

3. Нажмите **[Войти]**.

После успешного входа в систему откроется интерфейс портала администрирования.

Если несколько раз были введены неверный логин, пароль или одноразовый код, то учетная запись может быть заблокирована. Для разблокировки обратитесь к системному администратору. Количество попыток входа можно

настроить в разделе,.

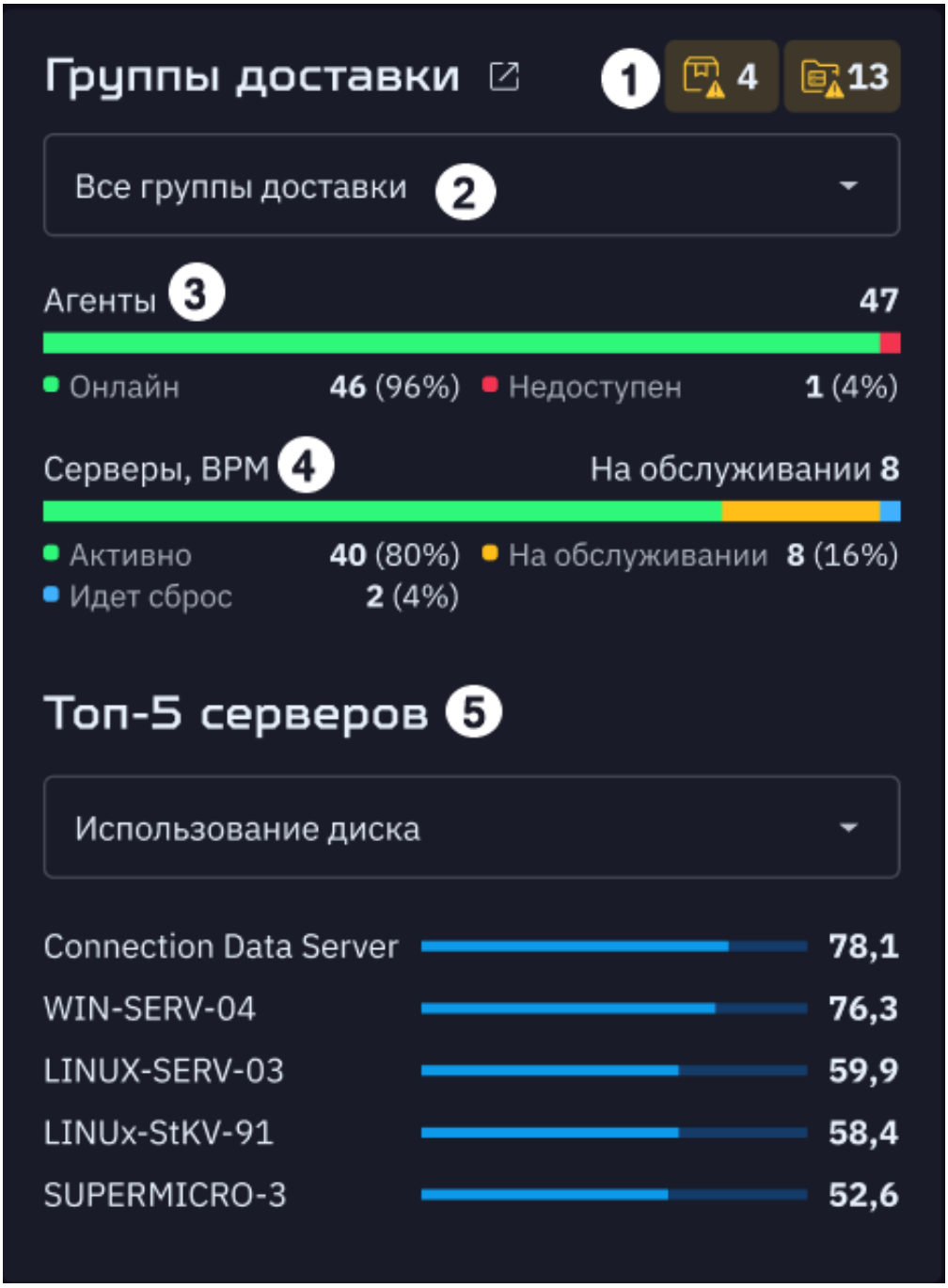
Глава 2. Обзор

В разделе **Обзор** можно посмотреть сводку о состоянии групп доставки, серверов, пользователей, приложений и компонентов брокера без дополнительного перехода в разделы портала администрирования.

Группы доставки

В этом блоке отображается информация о всех ресурсах для всех групп доставки, с возможностью ознакомиться с состоянием ресурсов для конкретной группы доставки.

Для детального ознакомления и настройки группы доставки перейдите в раздел **Группы доставки**, нажав .



1. Блок уведомлений

   В правом верхнем углу блока отображаются уведомления о состоянии ресурсов:

   - - уведомления для агентов. При наведении курсора на уведомление система выводит всплывающее сообщение. Примеры сообщений:
     - «Устаревшие агенты: N».
     - «Агенты не установлены: N».
     - «Агенты не поддерживают протокол X2Go: N».
     - «Агенты не поддерживают протокол RDP: N».
     - «Агенты не поддерживают подключение через веб-клиент: N».

       где N - количество агентов.

- - уведомления для групп доставки. При наведении курсора на уведомление система выводит всплывающее сообщение. Примеры сообщений:
  - «Группа доставки без приложений: N».
  - «Группа доставки без серверов: N».

  где N - количество групп доставки.

1. Значение метрик не зависит от выбранной группы доставки. Значение считается всегда для всех групп.
2. Уведомления отображаются только при наличии новых событий.

2. Поле выбора группы доставки.

   В выпадающем списке можно выбрать группу доставки, о которой необходимо посмотреть информацию.

3. Распределение агентов по статусам

   Ознакомиться со статусами агентов можно в таблице ниже:

   Таблица 1. Описание статусов агентов

Статус	**Описание**
Онлайн	Агент, установленный на сервере, периодически сообщает свой статус брокеру
Недоступен	Агент не отвечает на запросы сервера

   Для детального ознакомления и настройки агента перейдите в раздел.

4. Распределение серверов (ТС) по статусам

   Ознакомиться со статусами серверов (ТС) можно в таблице ниже:

   Таблица 2. Описание статусов ТС

Статус доступности	**Описание**
Активно	Сервер принимает пользовательские подключения и обеспечивает запуск приложений
На обслуживании	К серверу нельзя подключиться, но существующие сессии активны
Идет сброс	Выполняется сброс сессионной ВМ, любые операции над ВМ (изменение статуса, управление питанием) недоступны до завершения сброса

5. Виджет Топ-5 серверов

Виджет «Топ-5 серверов» показывает серверы с указанием имени группы доставки и объемом используемой памяти. Можно выбрать и посмотреть следующую информацию:

- **Использование RAM**

  При выборе значения **Использование RAM** отображается список топ-5 ТС с максимальной утилизацией по RAM в процентном соотношении.

- **Использование CPU**

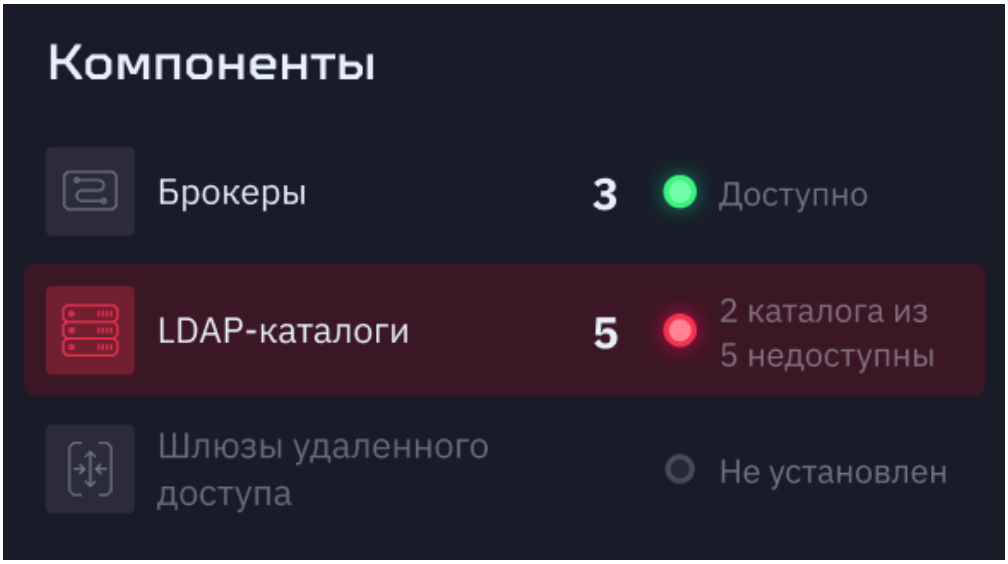
  При выборе значения **Использование CPU** отображается список топ-5 ТС с максимальной утилизацией по CPU в процентном соотношении.

- **Использование диска**

  При выборе значения **Использование диска** отображается список топ-5 ТС с максимальной нагрузкой по количеству использования диска.

Компоненты

Блок «Компоненты» показывает информацию о статусах доступности и количестве подключенных компонентов для оперативного реагирования на инциденты.



Для мониторинга доступны следующие компоненты:

- **Брокеры**. Чтобы посмотреть подробную информацию о брокере, нажмите на строку **Брокеры** для перехода в раздел **Брокеры** на портале администрирования.
- **LDAP-каталоги**. Чтобы посмотреть подробную информацию о LDAP-каталогах, нажмите на строку **LDAP-каталоги** для перехода в раздел **LDAP-каталоги**.

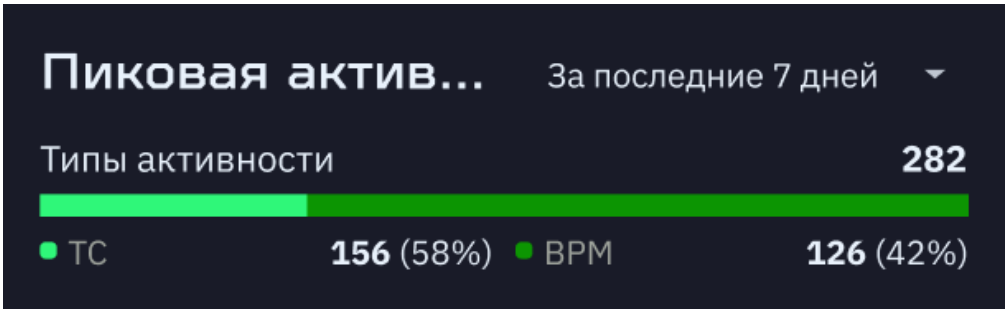
- **Шлюзы удаленного доступа**. Чтобы посмотреть подробную информацию о шлюзах удаленного доступа, нажмите на строку **Шлюз удаленного доступа** для перехода в раздел **Внешний доступ** с информацией о шлюзе удаленного доступа.

В данной таблице описаны статусы состояния компонентов:

Статус	Описание
Доступно	Компонент доступен и работоспособен, без зафиксированных ошибок доступности
Недоступен	Компонент добавлен в системе, но в данный момент недоступен или не отвечает (например, из-за сетевой недоступности или сбоя в работе)
Не установлен	Компонент не установлен в системе и не добавлен в брокере

Пиковая активность

В блоке **Пиковая активность** отображается максимальное количество пользователей, работающих в системе одновременно за выбранное количество времени. Данная метрика может дать пользователю с ролью **Администратор** примерную оценку, сколько конкурентных пользовательских лицензий в будущем может понадобиться.

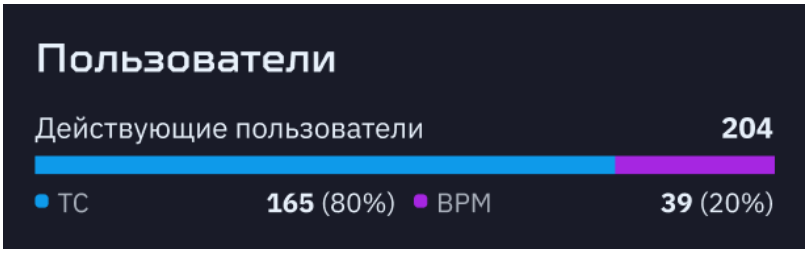


В расчет за период попадают активные, отключенные, открывающиеся сессии.

В правом верхнем углу блока можно выбратьпериод отображения данных за последние: 15 минут, 30 минут, час, сутки и 7 дней.

Пользователи

Блок содержит информацию об активных и неудаленных пользователях , которые хоть раз осуществляли подключение к ресурсам. Метрика является индикатором для сопоставления с именными лицензиями, которые могут понадобиться в будущем.

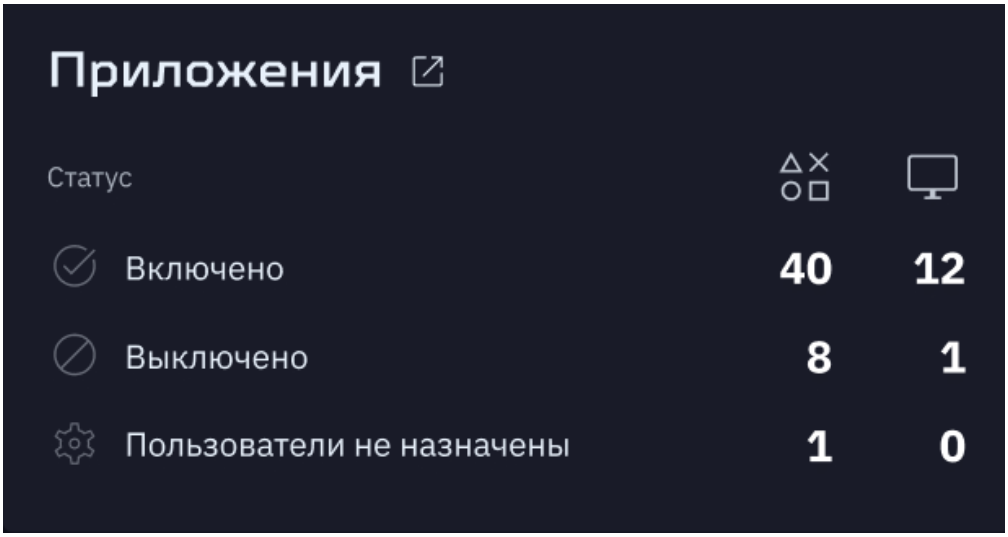


Даёт быстрый индикатор нагрузки с точки зрения количества активных пользователей, чтобы сопоставить её с ресурсами серверов и лицензиями.

1. Если у пользователя за все время работы в Termit было несколько сессий ТС, в расчете метрики пользователь будет учтен как 1 пользователь.
2. Если у пользователя никогда не было сессий в Termit, то в расчете метрики он не учитывается.

Приложения

Блок **Приложения** содержит сведения о добавленных приложениях и рабочих столах в Termit.



В блоке можно посмотреть информацию о:

- - количестве приложений.
- - количестве рабочих столов.

В данной таблице описаны статусы состояний приложений/рабочих столов:

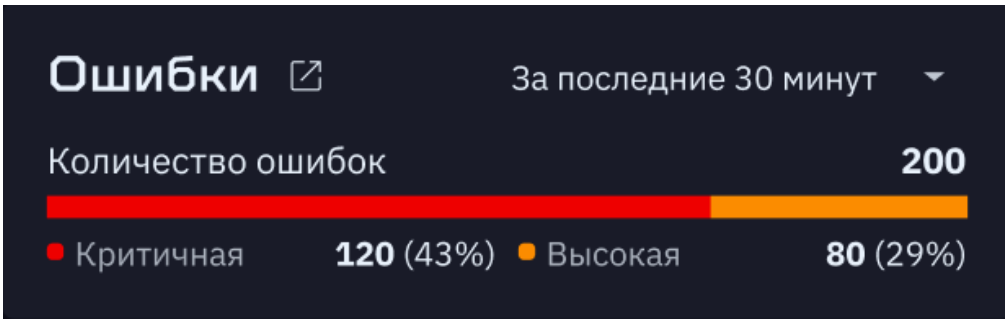
Статус	**Описание**
Включено	Количество приложений/рабочих столов статусе «Включено»
Выключено	Количество приложений/рабочих столов статусе «Выключено»

Статус	Описание
Пользователи не назначены	Количество приложений/рабочих столов, которые не назначены ни одной группе пользователей, т.е. ни один пользователь не имеет возможности запустить приложение/рабочий стол

Для детального ознакомления и настройки приложений/рабочих столов перейдите в раздел **Приложения**, нажав .

Ошибки

В блоке **Ошибки** отображается количество событий в системе с важностью **Критическая** и **Высокая** за выбранное количество времени.



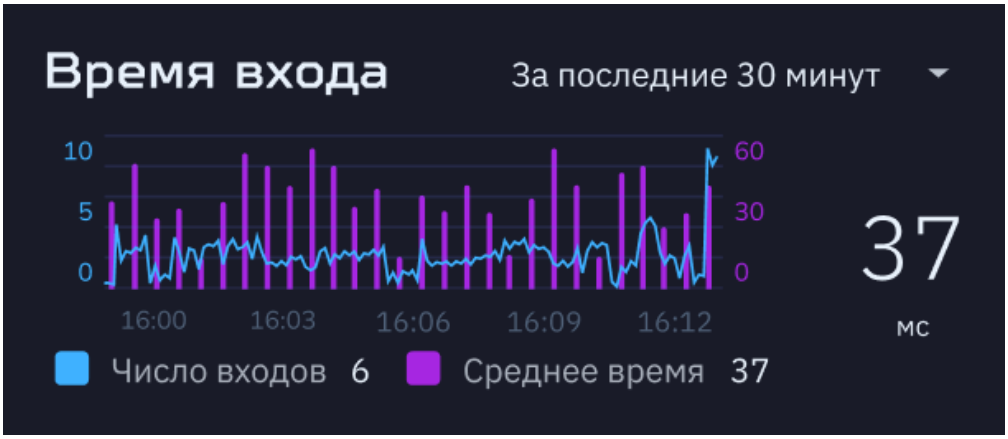
В правом верхнем углу блока можно выбрать период отображения данных за последние: 15 минут, 30 минут, час, сутки или 7 дней.

Для подробного ознакомления с ошибками перейдите в раздел **Журнал событий**, нажав .

При переходе в раздел события из раздела **Обзор** в раздел **События** записи автоматически отображаются с применёнными фильтрами: **Тип события** = «Ошибка», **Важность** = «Критичная» и «Высокая».

Время входа

В блоке **Время входа** отображается информация о среднем времени создания сессии до момента, когда сессия стала активной, что демонстрирует скорость обработки подключений пользователей.



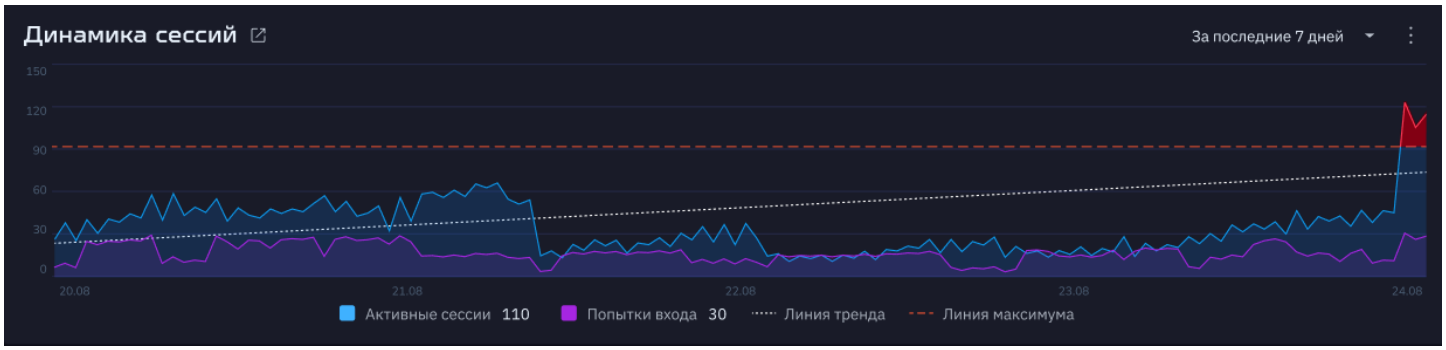
На графике отображается количество успешных подключений (успешно открытых сессий) пользователей. Учитываются сессии, которые одновременно удовлетворяют двум условиям:

- начали запускаться с начала выбранного периода и до его окончания;
- закончили запускаться на момент сбора данных.

В правом верхнем углу блока можно выбрать период отображения данных за последние: 15 минут, 30 минут, час, сутки или 7 дней.

Динамика сессий

Блок **Динамика сессий** содержит информацию о количестве попыток открыть сессию (попыток входа) и успешно установленных сессий (активные сессии).



В блоке **Динамика сессий** можно:

- регулировать период отображения данных.
- настроить линию максимума, превышение которой будет подсвечиваться, показывая наплыв пользователей.
- добавить/отключить линию максимума/линию тренда в графике. Линия тренда показывает динамику изменения нагрузки на систему за выбранный период, прогнозирует поведение системы.

В правом верхнем углу блока можно выбрать один из периодов времени для обзора

информации: за последние 15 минут, 30 минут, час, сутки и 7 дней.

Для настройки линии максимума:

- В правом верхнем углу блока нажмите ⋮.
- Нажмите **Настройки**.
- В поле **Значение линии максимума** заполните значение линии максимума.
- Нажмите **Сохранить**.

Значение линии максимума будет установлено.

Для того чтобы добавить/отключить линию максимума/линию тренда:

- В правом верхнем углу блока нажмите ⋮.
- Нажмите **Линия максимума**/**Линия тренда**.

Линия максимума/линия тренда будут добавлены/отключены из графика **Динамика сессий**.

Глава 3. Журнал событий

В журнале событий отображаются все операции, происходящие в системе. Это позволяет отслеживать несанкционированные действия. Кроме того, вы можете очищать старые записи журнала событий. Подробнее об этом в разделе Глубина хранения журналов,.

В разделе **Журнал событий** можно:

- найти нужное событие, нажав , по следующим признакам:
  - дате,
  - важности,
  - типу события,
  - категории,
  - инициатору,
  - компоненту,
  - учетной записи,
  - группе доставки,
  - адресу сервера,
  - приложению,
  - ID сессии.
- обновить список пользователей, нажав ;
- настроить видимость столбцов, нажав ;
- экспортировать данные в CSV, нажав ⋮ .

Список событий

Ниже представлен список событий, регистрируемых в системе Termit.

Таблица 3. События

Текст события	Важность	Статус	Категория
Не удалось стартовать сервер Termit. Имя сервера: {0}. Причина: {1}	Критическая	Ошибка	Системное
Не удалось выполнить синхронизацию с LDAP. Имя LDAP-каталога: {2}. Адрес LDAP-сервера: {0}. Причина: {1}	Критическая	Ошибка	Фоновые задачи
Не удалось выполнить инкрементальную синхронизацию с LDAP. Имя LDAP-каталога: {2}. Адрес LDAP-сервера: {0}. Причина: {1}	Критическая	Ошибка	Фоновые задачи

Текст события	Важность	Статус	Категория
Ошибка при аутентификации пользователя. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}	Высокая	Ошибка	Аутентификация
Ошибка при смене пароля пользователя. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}. Причина: {3}	Высокая	Ошибка	Аутентификация
Не удалось заблокировать учетную запись пользователя. ID пользователя: {0}. Причина: {1}	Высокая	Ошибка	Аутентификация
Не удалось разблокировать учетную запись пользователя. Имя пользователя: {0}. Причина: {1}	Высокая	Ошибка	Аутентификация
Не удалось разблокировать встроенную учетную запись пользователя. Имя пользователя: {0}. Причина: {1}	Высокая	Ошибка	Аутентификация
Доступ к объекту запрещён. Имя пользователя: {0}, Тип объекта: {1}, Операция: {2}	Высокая	Ошибка	Аутентификация
Не удалось открыть сессию для опубликованного приложения. ID приложения: {0}. Причина: {1}	Высокая	Ошибка	Сессии
Не удалось переподключить сессию для опубликованного приложения. ID приложения: {0}. Причина: {1}	Высокая	Ошибка	Сессии
Не удалось принудительно завершить терминальную сессию. ID сессии: {0}. Причина: {1}	Высокая	Ошибка	Сессии
Не удалось получить файл подключения к теневой сессии. ID сессии: {0}. Причина: {1}	Высокая	Ошибка	Сессии
Не удалось принудительно остановить процесс экземпляра приложения. PID процесса: {0}. ID процесса экземпляра приложения: {1}. Причина: {2}	Высокая	Ошибка	Сессии
Не удалось запустить приложение на сервере. ID сессии: {0}. Причина: {1}	Высокая	Ошибка	Сессии
Не удалось подключить сетевой диск. Сетевой адрес: {0}. Локальное имя: {1}. ID сессии {2}. Причина: {3}	Высокая	Ошибка	Системное
Проверка сервиса Pulsar Server на сервере {0} завершена с ошибкой	Высокая	Ошибка	Системное
Проверка установки X2Go на сервере {0} завершена с ошибкой	Высокая	Ошибка	Системное
Проверка конфигурации компонентов X2Go на сервере {0} завершена с ошибкой: {1}	Высокая	Ошибка	Системное
Проверка настроек групповой политики {0} на сервере {1} завершена с ошибкой	Высокая	Ошибка	Системное
Не удалось добавить новую группу доставки. Тип группы: {0}. Имя группы: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось изменить настройки группы доставки. Имя группы: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить статус группы доставки. ID группы: {0}. Новый статус: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить группу доставки. ID группы: {0}. Причина: {1}	Высокая	Ошибка	Управление

Текст события	Важность	Статус	Категория
Не удалось добавить новый каталог ресурсов. Тип каталога: {0}. Имя каталога: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось изменить настройки каталога ресурсов. Имя каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Ошибка изменения статуса серверов каталога ресурсов. ID каталога: {0}. Новый статус: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить каталог ресурсов. ID каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось добавить новый сервер. Тип сервера: {0}. Адрес сервера: {1}. ID группы: {2}. Причина: {3}	Высокая	Ошибка	Управление
Не удалось изменить настройки сервера. ID сервера: {0}. ID группы: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось изменить статус сервера. ID сервера: {0}. Новый статус: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить сервер. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось сгенерировать команду установки агента на сервер. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось сгенерировать команду обновления агента на сервере. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось сгенерировать команду удаления агента на сервере. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось сгенерировать токен установки агента на сервер. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось опубликовать новое приложение. Имя приложения: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить настройки опубликованного приложения. Имя приложения: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить статус опубликованного приложения. ID приложения: {0}. Новый статус: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить опубликованное приложение. ID приложения: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить настройки. Название настроек: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось добавить политику доступа. ID приложения: {0}. Guid LDAP группы: {1}. Эффект: {2}. Причина: {3}	Высокая	Ошибка	Управление
Не удалось удалить политику доступа. ID политики доступа: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить пароль администратора системы. Причина: {0}	Высокая	Ошибка	Управление
Не удалось изменить имя администратора системы. Причина: {0}	Высокая	Ошибка	Управление
Не удалось отключить администратора системы. Причина: {0}	Высокая	Ошибка	Управление

Текст события	Важность	Статус	Категория
Не удалось удалить брокер. ID брокера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новую категорию приложений. Название категории: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось обновить категорию приложений. Название категории: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось удалить категорию приложений. ID категории: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новый LDAP-каталог. Имя LDAP-каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить LDAP-каталог. Имя LDAP-каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось удалить LDAP-каталог. ID LDAP-каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось обновить настройки Kerberos. Идентификатор LDAP-каталога: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новую политику. Имя политики: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось обновить политику. Имя политики: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось удалить политику. ID политики: {0}. Причина: {1}	Высокая	Ошибка	Управление
Приоритеты политик не удалось изменить. Причина: {0}	Высокая	Ошибка	Управление
Не удалось создать новый шлюз. Адрес шлюза: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось обновить шлюз. ID шлюза: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось удалить шлюз. ID шлюза: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить список привязанных пользователей. ID сервера: {0}. ID пользователей LDAP: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось добавить доверенный сертификат. Причина: {0}	Высокая	Ошибка	Управление
Не удалось удалить доверенный сертификат. ID сертификата: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось открепить сервер от группы доставки. ID сервера: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось добавить новый сервер. Тип сервера: {0}. Адрес сервера: {1}. Имя каталога: {2}. Причина: {3}	Высокая	Ошибка	Управление
Не удалось выполнить экспорт страницы {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать задачу. Имя: {0}. ID группы доставки: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось изменить задачу. Имя задачи: {0}. ID задачи: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить задачу. ID задачи: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось активировать задачу. ID задачи: {0}. Причина: {1}	Высокая	Ошибка	Управление

Текст события	Важность	Статус	Категория
Не удалось деактивировать задачу. ID задачи: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новую роль. Название роли: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить роль. Название роли: {0}, ID роли: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить роль. ID роли: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новую область видимости. Название области: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить область видимости. Название области: {0}, ID области: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить область видимости. ID области: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось создать новое назначение. Название назначения: {0}. Причина: {1}	Высокая	Ошибка	Управление
Не удалось изменить назначение. Название назначения: {0}, ID назначения: {1}. Причина: {2}	Высокая	Ошибка	Управление
Не удалось удалить назначение. ID назначения: {0}. Причина: {1}	Высокая	Ошибка	Управление
Инкрементальная синхронизация LDAP включена, но предыдущая синхронизация не позволяет сделать ее. Имя LDAP-каталога: {0}. Причина: {1}	Высокая	Ошибка	Фоновые задачи
Ошибка при выполнении задачи по группе доставки. ID задачи: {0}. Причина: {1}	Высокая	Ошибка	Фоновые задачи
Встроенная учетная запись пользователя была заблокирована. Имя пользователя: {0}	Высокая	Предупреждение	Аутентификация
Администратор принудительно завершил терминальную сессию. Адрес терминального сервера: {0}. ID сессии: {1}	Высокая	Предупреждение	Сессии
Администратор принудительно остановил процесс экземпляра приложения. Адрес терминального сервера: {0}. PID процесса: {1}. ID процесса экземпляра приложения: {2}	Высокая	Предупреждение	Сессии
Использование памяти журналом событий превысило заданный порог в {0}% и составляет {1}%. База данных: {2}	Высокая	Предупреждение	Системное
Новый центр сертификации для шлюзов создан	Высокая	Информация	Управление
Брокер удален. Имя брокера: {0}	Высокая	Информация	Управление
Новый центр сертификации для терминальных серверов создан	Высокая	Информация	Управление
Проверка доступности сервиса XRDP на сервере {0} завершена с ошибкой	Средняя	Ошибка	Системное
Проверка параметра Policy в конфигурации XRDP на сервере {0} завершена с ошибкой. Текущее значение Policy: {1}	Средняя	Ошибка	Системное
Создание нового центра сертификации для шлюзов завершилось с ошибкой. Причина: {0}	Средняя	Ошибка	Управление

Текст события	Важность	Статус	Категория
Создание нового центра сертификации для терминальных серверов завершилось с ошибкой. Причина: {0}	Средняя	Ошибка	Управление
Учетная запись пользователя была заблокирована администратором. Имя пользователя: {0}	Средняя	Предупреждение	Аутентификация
Аутентификация пользователя. Имя пользователя: {0}. Источник: {1}. Результат: {2}	Средняя	Предупреждение	Аутентификация
Пользователю требуется смена пароля. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}	Средняя	Предупреждение	Аутентификация
Инкрементальная синхронизация LDAP включена, но предыдущая синхронизация не позволяет сделать ее. Имя LDAP-каталога: {0}. Причина: {1}, будет использоваться полная синхронизация	Средняя	Предупреждение	Фоновые задачи
Пользователь был успешно аутентифицирован. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}	Средняя	Информация	Аутентификация
Пользователь вышел из системы. Имя пользователя: {0}. Источник: {1}	Средняя	Информация	Аутентификация
Пользователь успешно сменил пароль. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}	Средняя	Информация	Аутентификация
Учетная запись пользователя была разблокирована администратором. Имя пользователя: {0}	Средняя	Информация	Аутентификация
Встроенная учетная запись пользователя была разблокирована. Имя пользователя: {0}	Средняя	Информация	Аутентификация
Ошибка при автоматической аутентификации пользователя. Имя пользователя: {0}. Источник: {1}. Тип входа: {2}	Средняя	Информация	Аутентификация
Успешно открыта сессия для опубликованного приложения. Адрес терминального сервера: {0}. Название приложения: {1}. ID сессии: {2}	Средняя	Информация	Сессии
Успешное переподключение сессии для опубликованного приложения. Адрес терминального сервера: {0}. Название приложения: {1}. ID сессии: {2}	Средняя	Информация	Сессии
Администратор запросил подключение к теневой сессии. Адрес сервера: {0}. ID сессии: {1}	Средняя	Информация	Сессии
Терминальная сессия была запущена на сервере. ID сессии: {0}	Средняя	Информация	Сессии
Терминальная сессия была завершена на сервере. Адрес терминального сервера: {0}. ID сессии: {1}	Средняя	Информация	Сессии
Пользователь отключился от терминальной сессии. Адрес терминального сервера: {0}. ID сессии: {1}	Средняя	Информация	Сессии
Агент с сервера {0} успешно зарегистрирован на брокере	Средняя	Информация	Системное
Сессия принудительно закрыта по таймауту. Адрес терминального сервера: {0}, ID сессии: {1}	Средняя	Информация	Системное
Сессия принудительно отключена по таймауту. Адрес терминального сервера: {0}, ID сессии: {1}	Средняя	Информация	Системное
Сетевой диск успешно подключён. Сетевой адрес: {0}. Локальное имя: {1}. ID сессии {2}	Средняя	Информация	Системное

Текст события	Важность	Статус	Категория
Сервер Termit стартовал. Имя сервера: {0}	Средняя	Информация	Системное
Сервер Termit остановлен. Имя сервера: {0}	Средняя	Информация	Системное
Старые записи аудита удалены. Количество: {0}, период с {1} по {2} (Время в UTC). База данных: {3}	Средняя	Информация	Системное
Старые закрытые сессии удалены. Количество: {0}, период с {1} по {2}	Средняя	Информация	Системное
Агент шлюза успешно стартовал {0}	Средняя	Информация	Системное
Старые записи аудита удалены. Количество: {0}. База данных: {1}	Средняя	Информация	Системное
Проверка сервиса Pulsar Server на сервере {0} завершена успешно	Средняя	Информация	Системное
Проверка установки X2Go на сервере {0} завершена успешно	Средняя	Информация	Системное
Проверка конфигурации компонентов X2Go на сервере {0} завершена успешно	Средняя	Информация	Системное
Проверка настроек групповой политики {0} на сервере {1} завершена успешно	Средняя	Информация	Системное
Проверка доступности сервиса XRDP на сервере {0} завершена успешно	Средняя	Информация	Системное
Проверка параметра Policy в конфигурации XRDP на сервере {0} завершена успешно	Средняя	Информация	Системное
Добавлена новая группа доставки. Тип группы: {0}. Имя группы: {1}	Средняя	Информация	Управление
Изменены настройки группы доставки. Тип группы: {0}. Имя группы: {1}	Средняя	Информация	Управление
Изменён статус группы доставки. Тип группы: {0}. Имя группы: {1}. Новый статус: {2}	Средняя	Информация	Управление
Удалена группа доставки. Тип группы: {0}. Имя группы: {1}	Средняя	Информация	Управление
Добавлен новый каталог ресурсов. Тип каталога: {0}. Имя каталога: {1}	Средняя	Информация	Управление
Изменены настройки каталога ресурсов. Тип каталога: {0}. Имя каталога: {1}	Средняя	Информация	Управление
Запрос изменения статуса серверов каталога ресурсов. ID каталога: {0}. Новый статус: {1}. (В перезагрузке: {2}, ошибок: {3})	Средняя	Информация	Управление
Удален каталог ресурсов. Тип каталога: {0}. Имя каталога: {1}	Средняя	Информация	Управление
Добавлен новый сервер. Тип сервера: {0}. Адрес сервера: {1}. Имя группы: {2}	Средняя	Информация	Управление
Изменены настройки сервера. Тип сервера: {0}. Адрес сервера: {1}	Средняя	Информация	Управление
Изменён статус сервера. Тип сервера: {0}. Адрес сервера: {1}. Новый статус: {2}	Средняя	Информация	Управление
Удален сервер. Тип сервера: {0}. Адрес сервера: {1}	Средняя	Информация	Управление

Текст события	Важность	Статус	Категория
Сгенерирована новая команда установки агента на сервер. Адрес сервера: {0}	Средняя	Информация	Управление
Сгенерирована команда обновления агента на сервере. Адрес сервера: {0}	Средняя	Информация	Управление
Сгенерирована команда удаления агента на сервере. Адрес сервера: {0}	Средняя	Информация	Управление
Сгенерирован токен установки агента на сервере: {0}	Средняя	Информация	Управление
Опубликовано новое приложение. Имя приложения: {0}	Средняя	Информация	Управление
Изменены настройки опубликованного приложения. Имя приложения: {0}	Средняя	Информация	Управление
Изменён статус опубликованного приложения. Имя приложения: {0}. Новый статус: {1}	Средняя	Информация	Управление
Удалено опубликованное приложение. Имя приложения: {0}	Средняя	Информация	Управление
Настройки были изменены. Название настроек: {0}	Средняя	Информация	Управление
Добавлена политика доступа. Имя приложения: {0}. Имя LDAP группы: {1}. Имя каталога: {3}. Эффект: {2}	Средняя	Информация	Управление
Удалена политика доступа. Имя приложения: {0}. Имя LDAP группы: {1}. Имя каталога: {3}. Эффект: {2}	Средняя	Информация	Управление
Пароль администратора системы изменён	Средняя	Информация	Управление
Имя администратора системы изменено	Средняя	Информация	Управление
Администратор системы отключен	Средняя	Информация	Управление
Добавлена новая категория приложений. Название категории: {0}	Средняя	Информация	Управление
Категория приложений была обновлена. Название категории: {0}	Средняя	Информация	Управление
Категория приложений была удалена. Название категории: {0}	Средняя	Информация	Управление
Создан новый LDAP-каталог. Имя LDAP-каталога: {0}	Средняя	Информация	Управление
Изменен LDAP-каталог. Имя LDAP-каталога: {0}	Средняя	Информация	Управление
Удален LDAP-каталог. Имя LDAP-каталога: {0}	Средняя	Информация	Управление
Настройки Kerberos были обновлены. Имя LDAP-каталога: {0}	Средняя	Информация	Управление
Создана новая политика. Имя политики: {0}	Средняя	Информация	Управление
Политика обновлена. Имя политики: {0}	Средняя	Информация	Управление
Политика удалена. ID политики: {0}	Средняя	Информация	Управление
Приоритеты политик были изменены	Средняя	Информация	Управление
Добавлен новый шлюз. Адрес шлюза: {0}	Средняя	Информация	Управление
Шлюз был обновлен. Адрес шлюза: {0}	Средняя	Информация	Управление
Шлюз был удален. Адрес шлюза: {0}	Средняя	Информация	Управление

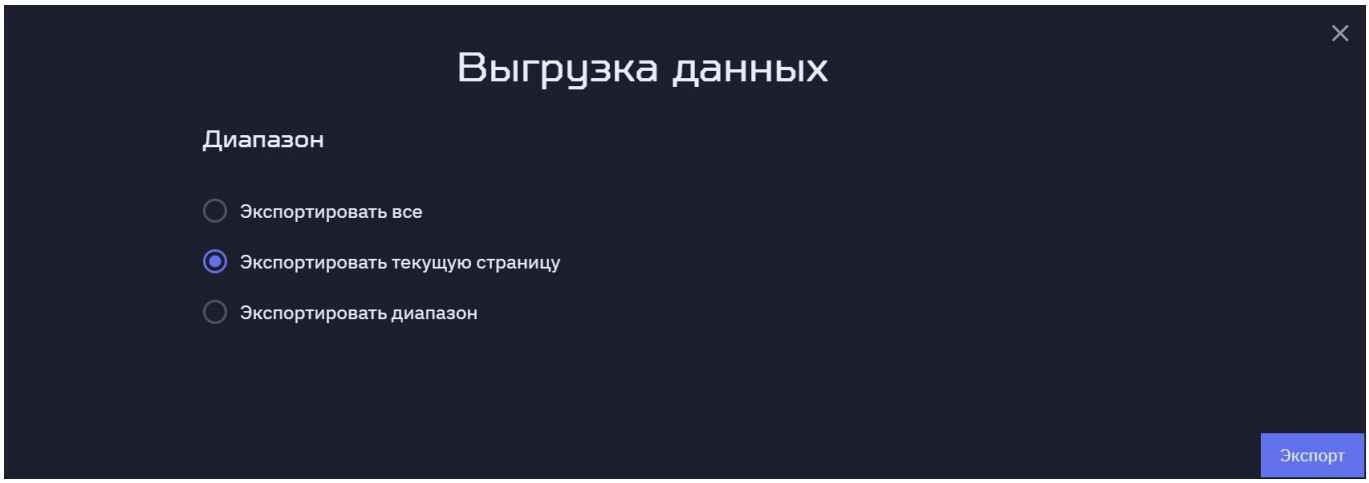
Текст события	Важность	Статус	Категория
Изменён список привязанных пользователей. Адрес {0}: {1}. ID пользователей LDAP: {2}	Средняя	Информация	Управление
Добавлен новый доверенный сертификат. CN: {0}	Средняя	Информация	Управление
Доверенный сертификат удален. Серийный номер: {0}, ID сертификата: {1}	Средняя	Информация	Управление
Сервер откреплен от группы доставки. Тип сервера: {0}. Адрес сервера: {1}	Средняя	Информация	Управление
Добавлен новый сервер. Тип сервера: {0}. Адрес сервера: {1}. Имя каталога: {2}	Средняя	Информация	Управление
Выполнен экспорт страницы {0}	Средняя	Информация	Управление
Создана задача. Имя задачи: {0}. Группа доставки: {1}	Средняя	Информация	Управление
Изменена задача. Имя задачи: {0}. Группа доставки: {1}	Средняя	Информация	Управление
Удалена задача. ID задачи: {0}	Средняя	Информация	Управление
Задача активирована. Имя задачи: {0}. Группа доставки: {1}	Средняя	Информация	Управление
Задача деактивирована. Имя задачи: {0}. Группа доставки: {1}	Средняя	Информация	Управление
Добавлена новая роль. Название роли: {0}	Средняя	Информация	Управление
Роль изменена. Название роли: {0}, ID роли: {1}	Средняя	Информация	Управление
Роль удалена. ID роли: {0}	Средняя	Информация	Управление
Добавлена новая область видимости. Название области: {0}	Средняя	Информация	Управление
Область видимости изменена. Название области: {0}, ID области: {1}	Средняя	Информация	Управление
Область видимости удалена. ID области: {0}	Средняя	Информация	Управление
Добавлено новое назначение. Название назначения: {0}	Средняя	Информация	Управление
Назначение изменено. Название назначения: {0}, ID назначения: {1}	Средняя	Информация	Управление
Назначение удалено. ID назначения: {0}	Средняя	Информация	Управление
Завершена синхронизация с LDAP. Имя LDAP-каталога: {2}. Адрес LDAP-сервера: {0}. Потрачено времени (сек): {1}, добавлено записей: всего {3}, групп {6}, пользователей {7}, обновлено записей: всего {4}, групп {8}, пользователей {9}, удалено записей: всего {5}, групп {10}, пользователей {11}	Средняя	Информация	Фоновые задачи
Завершена инкрементальная синхронизация с LDAP. Имя LDAP-каталога: {2}. Адрес LDAP-сервера: {0}. Потрачено времени (сек): {1}, добавлено записей: всего {3}, групп {5}, пользователей {6}, обновлено записей: всего {4}, групп {7}, пользователей {8}	Средняя	Информация	Фоновые задачи
Выполнена задача для группы доставки. Имя задачи: {0}. Группа доставки: {1}	Средняя	Информация	Фоновые задачи
Начата синхронизация с LDAP. Имя LDAP-каталога: {1}. Адрес LDAP-сервера: {0}	Средняя	Информация	Фоновые задачи

Текст события	Важность	Статус	Категория
Начата инкрементальная синхронизация с LDAP. Имя LDAP-каталога: {1}. Адрес LDAP-сервера: {0}	Средняя	Информация	Фоновые задачи

Экспорт данных в CSV

Чтобы выполнить экспорт данных в CSV:

1. На портале администрирования в левом меню выберите раздел **Журнал событий**.
2. Нажмите кнопку ⋮.
3. Нажмите **[Экспорт CSV]**.
4. Выберите данные для экспорта.



5. Нажмите **[Экспорт]**.

Выбранные данные будут экспортированы в файл CSV-формата.

Глава 4. Каталоги ресурсов

Каталоги ресурсов — логическая группа терминальных серверов (ТС), созданная с одинаковыми характеристиками. Каталоги могут объединяться в группы доставки для централизованного управления подключением к ресурсам.

В разделе **Каталоги ресурсов** можно:

- Найти нужные серверы в каталоге ресурсов по имени, отфильтровать по ОС, форматам использования и количеству активных сессий, нажав .
- Обновить список каталогов ресурсов, нажав .
- Настроить видимость столбцов, нажав .

Виды каталогов ресурсов

В Termit каталоги ресурсов — это терминальные серверы.

Статусы и действия с каталогом ресурсов и серверами

Все доступные статусы серверов в каталогах ресурсов и действия над ними описаны на странице.

Просмотр информации о каталоге ресурсов

Чтобы просмотреть информацию о каталоге ресурсов:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Нажмите на имя нужного каталога ресурсов.

   На вкладке **Серверы** отображается список ТС, их FQDN, группа доставки, тип ОС, статус доступности, статус питания, версия агента, статус агента, пользователь, протокол(ы) и количество активных сессий.

   Также на этой вкладке доступны действия с ТС: перевод в режим «На обслуживании» (делает ресурс недоступным для подключений), а также удаление из каталога.

   На вкладке **Сессии** отображается список с подробной информацией о всех пользовательских сессиях. В списках сессий представлена информация о каждой созданной сессии в Termit, ее текущем статусе и принадлежности к определенной группе

доставки. Также есть возможность очистки истории закрытых сессий пользователей. Подробнее в разделе.

На вкладке **События** отображается список уведомлений, связанных с серверами, находящимися в этом каталоге ресурсов. Это позволяет отслеживать несанкционированные действия. Кроме того, вы можете очищать старые записи журнала событий. Подробнее в разделе.

4.1. Статусы и действия с каталогом ресурсов и серверами

В приведенной ниже таблице описаны статусы и действия, которые можно выполнить над серверами в каталогах ресурсов.

Таблица 4. Статусная модель

Операция над сервером	**ТС (базовый способ)**
Перевести на обслуживание	Да, если текущий статус у сервера «Активен»
Снять с обслуживания	Да, если текущий статус у сервера «Обслуживание»
Установить агент	Да
Обновить агент	Да
Удалить агент	Да
Удалить Операция по удалению сервера	Да

Перевод ТС на обслуживание

Когда ТС находится на обслуживании, можно проводить работы, например, по обновлению ПО. Чтобы перевести ТС на обслуживание:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Нажмите на имя нужного каталога.
3. Наведите курсор на нужный ТС и нажмите .
4. Нажмите **[Да]**.

После перевода сервера существующие сессии будут активны, новые не будут запущены. Каталогу серверу присваивается статус «На обслуживании».

Снятие ТС с обслуживания

Чтобы снять ТС с обслуживания:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Нажмите на имя нужного каталога.
3. Наведите курсор на нужный ТС и нажмите 🔧.
4. Нажмите **[Да]**.

ТС будет снят с обслуживания.

Работа с агентом

Установка агента

Команду по установке агента можно получить после создания терминального сервера. Для этого:

1. На портале администрирования в левом меню выберите раздел **Каталог ресурсов**.
2. Наведите курсор на нужный каталог ресурсов.
3. Наведите курсор на нужный сервер и нажмите на FQDN сервера.
4. В правом верхнем углу нажмите ⋮.
5. Выберите **Установить агент**.
6. Скопируйте команду и выполните ее на терминальном сервере.

Агент будет установлен на терминальный сервер, и его статус изменится на «Онлайн».

Установка в ЗПС

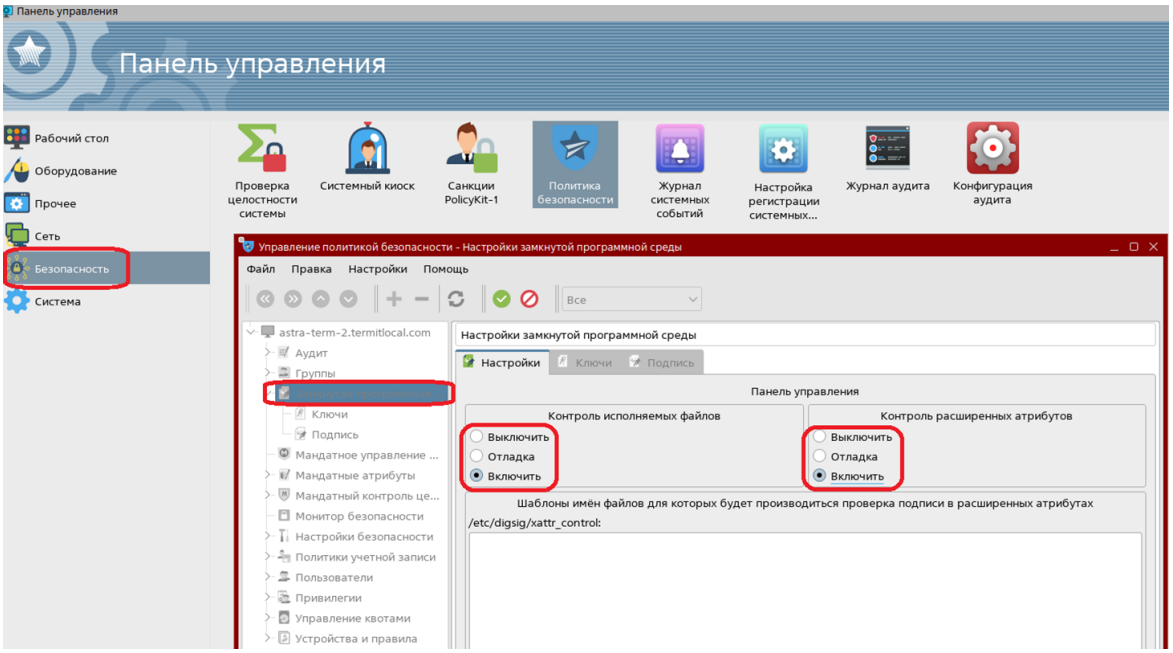
1. Перед установкой поместите публичный (открытый) ключ https://%АДРЕС_БРОКЕРА_ИЛИ_БАЛАНСИРОВЩИКА%/dist/termit_astra.key в директорию `/etc/digsig/keys` с помощью команды:

```
sudo cp %Путь_к_Открытому_Ключу% /etc/digsig/keys
```

2. Обновите ключи с помощью команды:

```
sudo update-initramfs -u -k all
```

3. Перезагрузите ПК.
4. Включите режим замкнутой программой среды (ЗПС), если не был включен ранее:



5. Установите агент в обычном режиме.

   При отображении «Ошибка сегментирования» ключ не может быть считан.

Ручное обновление агента

Чтобы обновить агент вручную:

1. На портале администрирования в левом меню выберите раздел **Каталог ресурсов**.
2. Наведите курсор на нужный каталог ресурсов.
3. Наведите курсор на нужный сервер и нажмите на FQDN сервера.
4. В правом верхнем углу нажмите ⋮.
5. Выберите **Обновить агент**.
6. Скопируйте команду и выполните ее на терминальном сервере.

Агент обновлен на терминальном сервере.

Удаление агента

Чтобы удалить агент:

1. На портале администрирования в левом меню выберите раздел ***Каталог ресурсов**.

2. Наведите курсор на нужный каталог ресурсов.
3. Наведите курсор на нужный сервер и нажмите на FQDN сервера.
4. В правом верхнем углу нажмите **[Дополнительно]**.
5. Выберите ⋮ .
6. Скопируйте актуальную команду на портале администрирования или предложенную ниже:
   - Для Linux:

     ```
     sudo ./agent-installer uninstall
     ```

   - Для Windows

     ```
     .\agent-installer.exe uninstall
     ```

7. Для Linux перейдите в каталог, где был запущен скрипт установки агента.

   Для Windows (операция удаления может быть выполнена только с правами администратора) перейдите по пути `C:\Program Files\TermitAgent\`.

8. Выполните скопированную команду в терминале.

Агент удален на терминальном сервере.

Удаление сервера из каталога ресурсов

Чтобы удалить сервер из каталога ресурсов:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Нажмите на имя нужного каталога ресурсов с серверами.
3. Наведите курсор на нужный сервер и нажмите ⋮ .
4. Нажмите **[Удалить сервер]**.

Сервер будет удален из каталога ресурсов.

Удаление каталога ресурсов

1. Нельзя удалить каталог, созданный базовым способом, если в него добавлены серверы. Подробнее в разделе Изменение настроек

терминальных серверов. При удалении серверов

2. Перед удалением каталога необходимо перевести все серверы в режим «На обслуживании».
3. Перед удалением каталога ресурсов на нем должны быть завершены все сессии.

Чтобы удалить каталог ресурсов:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Наведите курсор на нужный каталог и нажмите ⋮.

   Или нажмите на имя каталога ресурсов и в правом верхнем углу нажмите ⋮.
3. Нажмите **[Удалить каталог]**.
4. Нажмите **[Да]**.

Каталог ресурсов удален.

4.2. Терминальные серверы

Терминальный сервер (ТС) — сервер, который предоставляет доступ к ресурсам компьютера или сервера пользователям через десктоп- или веб-клиент. Пользователи могут подключаться к терминальному серверу и работать с приложениями, например 1С, данными и другими ресурсами, как если бы они работали непосредственно на сервере.

Каталог ресурсов формата **ТС** объединяет терминальные серверы с одинаковыми настройками. Наличие нескольких серверов в каталоге позволяет балансировать нагрузку и обеспечивает отказоустойчивость.

На странице **Каталоги ресурсов** для формата **ТС** можно:

- Найти нужные серверы на вкладке **Серверы** по имени, типу ОС, статусу доступности, статусу агента, пользователю и активным сессиям, нажав ⏷.
- Обновить список серверов, нажав ↻.
- Настроить видимость столбцов, нажав ▥.

Создание каталога ресурсов

Каталог ресурсов формата **ТС** создается базовым способом. Серверы добавляются на

вкладке **Добавление серверов** в процессе создания каталога.

Базовый

Чтобы создать каталог ресурсов формата **TC** базовым способом:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. В правом верхнем углу нажмите **[Создать каталог>TC]**.
3. На вкладке **Общие настройки**:
   - **Имя** — задайте имя каталога ресурсов.
   - **Тип ОС** — выберите операционную систему **Linux** или **Windows**.
   - (Опционально) **Описание** — добавьте описание каталога серверов.
4. Нажмите **[Далее]**.
5. На вкладке **Способ создания** выберите способ создания каталога серверов - **Базовый**.
6. Нажмите **[Далее]**.
7. На вкладке **Добавление серверов** можно настроить, какие серверы доступны пользователям в каталоге ресурсов:
   - Нажмите ＋.
   - Установите флажок в поле **FQDN сервера вручную** и задайте параметры:
     - **FQDN сервера** — укажите FQDN адрес терминального сервера.
     - Если имеется CSV-файл — установите флажок в поле **CSV-файл** и загрузите его в поле **Файл**.

     Максимальное количество строк: 100. Поддерживаемый формат: `.csv`.
8. Нажмите **Сохранить › Далее**.
9. На вкладке **Подтверждение** проверьте информацию о каталоге и нажмите **[Создать]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Созданный каталог ресурсов формата **TC** появится в списке.

Изменение настроек терминальных серверов

Чтобы изменить настройки каталога ресурсов формата **TC**:

1. На портале администрирования в левом меню выберите раздел **Каталоги ресурсов**.
2. Наведите курсор на нужный каталог формата **ТС** и нажмите ✎.
3. На вкладке **Общие настройки** измените параметры:

   Базовый

   - **Имя** — название каталога ресурсов.
   - (Опционально) **Описание** — измените описание каталога ресурсов.

   Затем нажмите **[Далее]** и перейдите на вкладку **Терминальные серверы**. Нажмите + и установите флажок в поле **FQDN сервера вручную** и задайте параметры:

   - **FQDN сервера** — укажите FQDN адрес терминального сервера.
   - Если имеется CSV-файл — установите флажок в поле **CSV-файл** и загрузите его в поле **Файл**.

     Максимальное количество строк: 100. Поддерживаемый формат: `.csv`.

   Нажмите **Сохранить** › **Далее** для перехода на следующую вкладку.

4. На вкладке **Подтверждение** проверьте информацию о каталоге ресурсов и нажмите **[Сохранить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Настройки каталога ресурсов формата **ТС** будут изменены.

Глава 5. Группы доставки

Группа доставки — это объединение ТС, выбранных из одного или нескольких каталогов ресурсов. Группа доставки определяет, какие пользователи могут использовать данные ресурсы, а также какие приложения и/или рабочие столы доступны этим пользователям.

Создание группы доставки является следующим шагом после установки системы терминального доступа и создания каталога ресурсов,.

В разделе **Группы доставки** можно:

- Найти нужные группы по имени, формату использования каталога ресурсов, типу ОС, активным сессиям и статусу доступности, нажав .
- Обновить список групп доставки, нажав .
- Настроить видимость столбцов, нажав .

Просмотр информации о группе доставки

Чтобы просмотреть информацию о группе доставки:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Нажмите на имя нужной группы доставки.
3. Нажмите на **Показать дополнительные параметры** для просмотра дополнительных параметров о группе доставки.

   На вкладке **Серверы** отображается список ТС, их FQDN, каталог ресурсов, тип ОС, статус доступности, версия агента, статус агента, пользователь, протокол(ы) и количество активных сессий.

   Также на этой вкладке можно перезагрузить, выключить/включить, или удалить ТС из группы доставки.

   На вкладке **Приложения** отображается список приложений, их названия и версия, статус.

   Также на этой вкладке можно включить и выключить приложение.

   На вкладке **Сессии** отображается список с подробной информацией о запущенных сессиях. В списках сессий представлена информация о каждой созданной сессии в Termit, ее текущем статусе и принадлежности к определенной группе доставки. Также есть возможность очистки истории закрытых сессий пользователей. Подробнее в разделе.

На вкладке **События** отображается список событий, связанных с этой группой доставки. Это позволяет отслеживать несанкционированные действия. Кроме того, вы можете очищать старые записи журнала событий. Подробнее в разделе.

Создание группы доставки

Чтобы создать группу доставки:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. В правом верхнем углу нажмите **[Создать группу]**.
3. На вкладке **Общие настройки**:
   - **Имя** — задайте имя группы доставки.
   - (Опционально) **Описание** — добавьте описание группы доставки.
   - **Формат использования** — **ТС**.
   - **Способ создания** — **базовый**.
   - **Тип ОС** — выберите операционную систему **Linux** или **Windows**.
4. Нажмите **[Далее]**.
5. На вкладке **Добавление каталогов и серверов**:
   - **Протокол подключения** — выберите протокол подключения **X2Go**, **RDP** или **Pulsar**.

Для ТС на ОС Linux доступны протоколы X2Go и Pulsar. Для ТС на ОС Windows доступен протокол RDP. Протокол используется для подключения через десктоп-клиент Termit.

   - Выберите каталоги ресурсов и количество добавленных серверов.
   - Нажмите **[Далее]**.
6. На вкладке **Подключение сетевых дисков** можно настроить, какие сетевые диски будут доступны пользователям в терминальной сессии. Подробнее о настройке,.
7. На вкладке **Таймауты сессий** выберите действия и время ожидания для активных, отключенных и бездействующих (нет активности пользователя) сессий:
   - **Ничего** — действия с сессиями выполняться не будут.
   - **Отключить** — сессия будет отключена по истечении указанного времени ожидания. При этом она не закроется, и приложения продолжат работать в фоновом режиме. Пользователь сможет заново к ним подключиться.

- **Завершить** — сессия будет закрыта по истечении указанного времени ожидания.

Подробнее о типах сессий,.

8. Нажмите **Сохранить** › **Далее**.
9. На вкладке **Подтверждение** проверьте информацию о группе доставке и нажмите **[Добавить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Созданная группа доставки появится в списке.

Подключение сетевых дисков

Чтобы настроить, какие сетевые диски будут доступны пользователям в терминальной сессии (группе доставки):

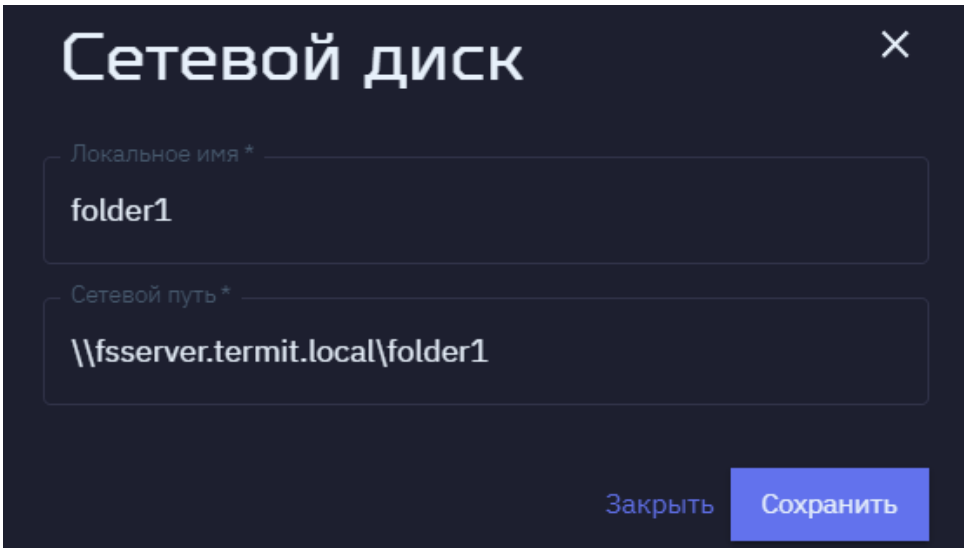
1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу и нажмите ✎.
3. Перейдите на вкладку **Подключение сетевых дисков**.
4. Нажмите +.
5. Задайте параметры:
   - **Локальное имя** — имя сетевого диска, которое будет отображаться у пользователя в терминальной сессии. Имя не должно содержать двух точек подряд `..`. В этом параметре:
     - для каталога ресурсов на базе Windows выберите из списка букву.
     - для каталога ресурсов на базе Linux укажите название подкаталога в домашнем каталоге пользователя, например `folder1`.
   - **Сетевой путь** — маршрут к сетевому файлу. Можно указать путь:
     - для общих дисков, которые будут доступны всем пользователям. Например:
       - на базе Windows в формате `\\FQDN\common-share`
       - на базе Linux в формате `\\FQDN\common-share`
     - для пользовательских дисков, которые будут доступны только конкретному пользователю. Например:
       - на базе Windows в формате `\\FQDN\user-shares\%USERNAME%`
       - на базе Linux в формате `\\FQDN\user-shares\$USER`

Пример заполнения

Windows

[s network disk windows] | *s__network-disk-windows.png*

Linux



6. Нажмите **Сохранить › Далее**.
7. На вкладке **Подтверждение** проверьте информацию о группе серверов и нажмите **[Сохранить]**.

Сетевые диски будут подключены.

Изменение группы доставки

Чтобы изменить настройки группы доставки:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу доставки и нажмите ✎.
3. На вкладке **Общие настройки** измените параметры:
   - **Имя** — название группы группы доставки.
   - (Опционально) **Описание** — измените описание группы доставки.
4. Нажмите **[Далее]** и перейдите на вкладку **Добавление каталогов и серверов** и внесите изменения:
   - Выберите каталоги ресурсов и/или увеличьте количество добавленных серверов.
5. Нажмите **[Далее]** для перехода на следующую вкладку.
6. На вкладке **Подключение сетевых дисков** измените параметры сетевых дисков. Для этого наведите курсор на нужный диск и нажмите ✎.

Чтобы добавить новый сетевой диск, нажмите ＋. Подробнее о настройке.

Чтобы удалить сетевой диск, наведите курсор на нужный диск и нажмите 🗑.

7. На вкладке **Таймауты сессий** измените действия и время ожидания для активных, отключенных и бездействующих (нет активности пользователя) сессий. Для этого наведите курсор на нужные поля и внесите изменения:
   - **Ничего** — действия с сессиями выполняться не будут.
   - **Отключить** — сессия будет отключена по истечении указанного времени ожидания. При этом она не закроется, и приложения продолжат работать в фоновом режиме. Пользователь сможет заново к ним подключиться.
   - **Завершить** — сессия будет закрыта по истечении указанного времени ожидания.

   Подробнее о типах сессий,.
8. Нажмите **[Далее]**.
9. На вкладке **Подтверждение** проверьте информацию о группе доставке и нажмите **[Сохранить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Настройки группы доставки будут изменены.

Перевод группы доставки в режим обслуживания

Когда группа доставки находится на обслуживании, можно проводить работы, например, по обновлению ПО. Чтобы перевести группу доставки в режим обслуживания:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу доставки и нажмите 🔧.
3. Нажмите **[Да]**.

После перевода в группе доставки существующие сессии будут активны, новые не будут запущены. Группе доставки будет присвоен статус «На обслуживании».

Вывод группы доставки из режима обслуживания

Чтобы снять группу доставки из режима обслуживания:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу доставки и нажмите .
3. Нажмите **[Да]**.

Группа доставки будет снята из режима обслуживания.

Отсоединение пользователя от сервера

Для отсоединения пользователя от сервера:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Нажмите на имя нужной группы.
3. Наведите курсор на нужный сервер и нажмите .
4. Нажмите **[Отсоединить]**.

   Для отмены действия нажмите **[Отменить]**.

На странице группы столбец **Пользователь** будет пустым. Пользователь будет откреплен от сервера. Любой пользователь сможет подключиться к данному серверу.

Управление задачами

- Необходимо контролировать отсутствие пересечений задач по времени при формировании расписания, так как автоматическая проверка наложений не выполняется.
- Уведомления о начале выполнения запланированных задач отсутствуют.

Чтобы настроить расписание выполнения операций со всеми серверами группы доставки:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу и нажмите ⋮.
3. Нажмите **[Настроить задачу]**.
4. В окне **Настройка задачи группы доставки**:
   - **Задача** — активируйте опцию, чтобы настроить выполнение задачи по расписанию.
   - **Имя задачи** — укажите имя задачи.
   - (Опционально) **Описание** — добавьте описание выполнения задачи.

- **Часовой пояс** — из выпадающего списка выберите часовой пояс, в котором будет выполняться задача по графику.
- **Действие** — из выпадающего списка выберите тип задачи:
  - **Перевести на обслуживание**,
  - **Снять с обслуживания**,
  - **Перезагрузить**,
  - **Сбросить**,
  - **Включить**,
  - **Завершить работу**,
  - **Завершить принудительно**.
- **Периодичность** — выберите периодичность выполнения задачи:
  - **Однократно**,
  - **Ежедневно**,
  - **Еженедельно**.
- **Параметры выполнения** — укажите параметры выполнения:

  Набор параметров зависит от выбранной периодичности.

  - **День недели**,
  - **Время**,
  - **Дата начала**,
  - (Опционально) **Дата завершения**.

5. Нажмите **[Сохранить]**.

   Задача будет добавлена в список запланированных задач.

Список запланированных задач будет виден на на вкладке **Группы доставки** › **Задачи**.

Чтобы посмотреть и, при необходимости, отредактировать список запланированных задач:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Нажмите на имя нужной группы.
3. Перейдите на вкладку **Задачи**.

   На вкладке будет отображаться список запланированных задач.

4. Чтобы отредактировать задачу:

a. Напротив нужной задачи нажмите ✎.
b. Измените параметры задачи и нажмите **[Сохранить]**.
c. Подтвердите изменения, нажав **[Изменить]**.

5. Чтобы удалить задачу:
   a. Напротив нужной задачи нажмите 🗑.
   b. Нажмите **[Удалить]**.

Удаление группы доставки без зависимостей

Нельзя удалить группу в статусе **Активна**. Чтобы продолжить, переведите ее в статус **На обслуживании**. Подробнее в разделе.

Чтобы удалить группу доставки без зависимостей:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу и нажмите ⋮.
3. Нажмите **[Удалить группу доставки]**.
4. Нажмите **[Удалить]**.

Группа доставки будет удалена.

Удаление группы доставки с зависимостями

Группы доставки с зависимостями - это группы доставки, на которые назначены приложения, пользователь или политики.

1. Нельзя удалить группу в статусе **Активна**. Чтобы продолжить, переведите ее в статус **На обслуживании**. Подробнее в разделе.
2. В случае, если удалить группу доставки с зависимостью, то:
   a. Приложения и серверы будут отсоединены от группы. Подробнее об отсоединении приложения и сервера от группы доставки (ссылка на статью)
   b. Группа доставки будет исключена из политик. Статус политик, применяемых только к этой группе, изменится на «Черновик». Подробнее об отсоединении политики от группы доставки (ссылка на статью)

Чтобы удалить группу доставки с зависимостями:

1. На портале администрирования в левом меню выберите раздел **Группы доставки**.
2. Наведите курсор на нужную группу и нажмите ⋮.
3. Нажмите **[Удалить группу]**.
4. Нажмите **[Удалить]**.

Группа доставки будет удалена.

Глава 6. Приложения

Приложение — это программное обеспечение или рабочий стол, запускаемые на ТС, интерфейс которых отображается на компьютере пользователя.

В разделе **Приложения** можно:

- Найти нужные приложения по имени, версии, наименованию у пользователя, группе серверов, статусу и типу, нажав .
- Обновить список приложений, нажав .
- Настроить видимость столбцов, нажав .
- Экспортировать данные в CSV, нажав .

Добавление приложения

Чтобы добавить приложение:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Нажмите **[Добавить приложение]**.
3. На вкладке **Общие настройки** задайте параметры:
   - **Имя** — название приложения.
   - **Тип ОС** — **Linux** или **Windows**.
   - **Тип** — выберите **Приложение** или **Рабочий стол**.

Чтобы в десктоп-клиенте приложения и рабочие столы отображались в отдельных списках, включите опцию **Разделение объектов на приложения и рабочие столы**, в настройках.

   - **Группа доставки** — выберите группы доставки или создайте новую в разделе **Группы доставки**,.
   - **Команда для запуска** — команда для запуска приложения или рабочего стола. Также для запуска приложения можно указать путь к исполняемому файлу и добавить параметры через пробел.

1. Короткую команду (вместо пути до исполняемого файла) можно использовать, если она позволяет запустить приложение напрямую на ТС, на который публикуется данное приложение. Например,

`chromium` (Linux) или `notepad.exe` (Windows).

2. Если путь к приложению содержит пробелы (например, в названии папки или файла), его необходимо заключить в кавычки для корректного выполнения команды, например `"/opt/My Programs/app"` (Linux) или `"C:\Program Files\Google\Chrome\Application\chrome.exe"` (Windows).
3. Публикуемые приложения Windows не поддерживают системные переменные окружения в командах.

- Команды для запуска рабочего стола:
  - Linux:
    - XFCE — `xfce4-session`
    - MATE — `mate-session`
    - FLY — `fly-wm`
- Команды для запуска приложений с графическим интерфейсом (например, Chromium/Chrome):
  - Linux:
    - Chromium — `chromium`
  - Windows:
    - Chrome — `"C:\Program Files\Google\Chrome\Application\chrome.exe"`
- Команды для запуска приложений без графического интерфейса (например, `top`):
  - Linux:
    - XFCE — `xfce4-terminal -e "top"`
    - MATE — `mate-terminal -e "top"`
    - FLY — `fly-term -e "top"`

◦ (Опционально) **Версия** — версия приложения.

◦ (Опционально) **Описание** — описание приложения.

4. Нажмите **[Далее]**.
5. На вкладке **Пользовательский вид** задайте настройки пользовательского отображения. Для этого:

◦ (Опционально) Загрузите иконку приложения.

1. Поддерживается только формат JPEG, другие форматы изображений не принимаются.

2. Максимальное допустимое к загрузке разрешение составляет 128x128 пикселей.

- (Опционально) **Имя у пользователя** — название приложения, которое будет отображаться у пользователя в десктоп-клиенте.
- (Опционально) Добавьте категорию приложения. Для этого:
  - Нажмите ＋.
  - Выберите категорию или создайте новую в разделе Категории, и нажмите **[Сохранить]**.

6. Нажмите **[Далее]**.
7. На вкладке **Группы доступа приложения** добавьте LDAP-группу и при необходимости задайте фильтр доступа к приложению::
   a. Нажмите ＋ и выберите из списка LDAP-группу, пользователи которой будут иметь доступ к этому приложению. Можно добавлять несколько групп доступа к приложению.
   b. (Опционально) Нажмите и задайте условия, при которых приложение будет доступно пользователю. Каждое условие — это строка с полями **Атрибут**, **Условие**, **Значение**:
      - **Атрибут** — выберите тип проверяемого параметра:
        - **Тип подключения** — определяет сетевую среду пользователя;
        - **Зона** — определяет отношение IP адреса клиентского устройства пользователя к Зоне (набору подсетей) в зависимости от выбранного условия.
      - Для атрибута **Тип подключения**:
        - **Условие** — выберите способ сравнения: **Равно** или **Не равно**;
        - **Значение** — выберите Зону из списка.
      - Для атрибута **Зона**:
        - **Условие** — выберите способ сравнения: **Находится** или **Не находится**;
        - **Значение** — выберите город из списка. Условие выполняется, если IP-адрес пользователя входит в маску подсети выбранного города.
      - (Опционально) **+ Добавить условие** — при необходимости добавьте еще одно условие.
      - (Опционально) **И** или **ИЛИ** — при добавлении второго и последующих условий, выберите логику объединения условий.

Порядок выполнения логических операций: сначала выполняются

операции с логическим И, затем - с логическим ИЛИ.

- Нажмите **[Применить]**.

c. Нажмите **[Добавить]**.

8. Нажмите **[Далее]**.
9. На вкладке **Подтверждение** проверьте информацию о приложении и нажмите **[Добавть]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

После создания приложение появится в списке со статусом «Включено». Приложение будет готово к работе.

Просмотр информации о приложении

Чтобы просмотреть информацию о приложении:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Наведите курсор на нужное приложение и нажмите на имя приложения.

На странице отобразятся сессии, события, категории и группы доставки, связанные с этим приложением.

Изменение параметров приложения

Чтобы изменить настройки приложения:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Наведите курсор на приложение и нажмите ✎.
3. На вкладке **Общие настройки** измените параметры:
   - **Имя** — название приложения.
   - **Тип** — выберите **Приложение** или **Рабочий стол**.

Чтобы в десктоп-клиенте приложения и рабочие столы отображались в отдельных списках, включите опцию **Разделение объектов на приложения и рабочие столы**, в настройках.

   - **Группа доставки** — выберите группы доставки или создайте новую в разделе **Группы доставки**,.

- **Команда для запуска** — команда для запуска приложения.

1. Короткую команду (вместо пути до исполняемого файла) можно использовать, если она позволяет запустить приложение напрямую на ТС, на который публикуется данное приложение. Например, `chromium` (Linux) или `notepad.exe` (Windows).
2. Если путь к приложению содержит пробелы (например, в названии папки или файла), его необходимо заключить в кавычки для корректного выполнения команды, например `"/opt/My Programs/app"` (Linux) или `"C:\Program Files\Google\Chrome\Application\chrome.exe"` (Windows).
3. Публикуемые приложения Windows не поддерживают системные переменные окружения в командах.

- (Опционально) **Версия** — версия приложения.
- (Опционально) **Описание** — описание приложения.

4. Нажмите **[Далее]**.
5. На вкладке **Пользовательский вид** измените настройки пользовательского отображения:
   - Удалите иконку приложения, нажав 🗑.
   - Загрузите иконку приложения.
   - (Опционально) **Название у пользователя** — название приложения, которое будет отображаться у пользователя в десктоп-клиенте.
   - (Опционально) Измените категорию приложения или добавьте новую.
6. Нажмите **[Далее]**.
7. На вкладке **Группа доставки** выберите группу доставки для приложения.
8. Нажмите **[Далее]**.
9. На вкладке **Группы доступа приложения** измените LDAP-группу или добавьте новую.
10. Нажмите **Добавить › Далее**.
11. На вкладке **Подтверждение** проверьте информацию о приложении и нажмите **[Сохранить]**.

Параметры приложения будут изменены.

Выключение приложения

Чтобы выключить приложение:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Наведите курсор на приложение и нажмите ⏻.
3. Нажмите **[Выключить]**.

Статус приложения изменится на «Выключено», оно станет недоступно пользователям.

Включение приложения

Чтобы включить приложение:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Наведите курсор на приложение и нажмите ⏻.
3. Нажмите **[Включить]**.

Статус приложения изменится на «Включено», оно станет доступно пользователям.

Удаление приложения

Чтобы удалить приложение:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Наведите курсор на приложение и нажмите ⋮.
3. Нажмите **[Удалить приложение]**.
4. Нажмите **[Да]**.

Приложение будет удалено.

Для отмены действия нажмите **[Отменить]**.

Скачивание файла подключения к ТС

Чтобы скачать файл подключения к ТС:

1. На портале администрирования в левом меню выберите раздел **Приложения**.

2. Наведите курсор на приложение и нажмите ⋮.
3. Нажмите **[Скачать файл]**.

Файл будет скачан на ПК. В файле подключения будут представлены все необходимые настройки для быстрого подключения к ТС: адрес сервера и ID приложения.

Экспорт данных в CSV

Чтобы выполнить экспорт данных в CSV:

1. На портале администрирования в левом меню выберите раздел **Приложения**.
2. Нажмите ⋮.
3. Нажмите **[Экспорт CSV]**.
4. Выберите данные для экспорта.
5. Нажмите **[Экспорт]**.

Выбранные данные будут экспортированы.

Ограничение запуска нескольких экземпляров приложений

Чтобы выставить ограничение на запуск нескольких экземпляров приложений требуется отправить запрос в API. Для этого в разделе **PATCH** `/api/v2/admin/resources/{id}` в параметре `max_instances_per_user` выставите значение `1`, где:

- `{id}`— id приложения.

Пример выставления ограничения через PATCH-запрос

```
curl --location --request PATCH
'https://<имя_брокера>/client/api/v2/admin/resources/<id_приложения>' \
--header 'Content-Type: application/json' \
--header 'Authorization: Bearer <токен>' \
--data '{
  "maxInstancesPerUser": 1
}'
```

- `<имя_брокера>` — имя брокера клиента. В адресе запроса это хост, например `internal.termit.local`.
- `<id_приложения>` — идентификатор вашего приложения. В адресе запроса это значение после `/resources/`.

- `<токен>` — токен авторизации. В заголовке `Authorization` он указывается после `Bearer`.

Глава 7. Сессии

В списках сессий представлена информация о каждой созданной сессии в Termit, ее текущем статусе и принадлежности к определенной группе доставки. Также есть возможность очистки истории закрытых сессий, пользователей.

В разделе **Сессии** можно:

- Найти нужную сессию, нажав .
- Обновить список сессий, нажав .
- Настроить видимость столбцов, нажав .
- Посмотреть подробную информацию о сессиях пользователей.
- Завершить сессии пользователей.
- Экспортировать данные в CSV, нажав .

Статусы сессий

Статус	Описание
Активная	Пользователь начал работу в сессии
Отключенная	Сессия активная, но пользователь к ней не подключен
Открывается	Сессия в процессе открытия
Закрывается	Сессия в процессе закрытия
Переподключается	Сессия в процессе повторного подключения пользователя
Закрытая	Сессия завершена
Отключается	Сессия в процессе отключения

Подключение в сессию сотрудника

Чтобы подключиться в сессию сотрудника:

1. На портале администрирования в левом меню выберите раздел **Сессии**.
2. Наведите курсор на нужную сессию в статусе **Активная** и нажмите .

   Файл для подключения к сессии пользователя будет скачан на ПК.

3. Откройте полученный файл в приложении Термит десктоп-клиент (termit-desktop) для подключения к сессии пользователя.

4. Пользователю придёт запрос на подключение к сессии, который он должен одобрить (Linux — **[Grant access]**, Windows — **[Да]**).

После подтверждения со стороны пользователя откроется окно с сессией пользователя.

Завершение сессии

Если пользователь подключен к серверу, который нужно выключить, например для обслуживания, то сессию можно завершить принудительно. Для этого:

1. На портале администрирования в левом меню выберите раздел **Сессии**.
2. Наведите курсор на активную или отключенную сессию и нажмите ⊠.
3. Нажмите **Да**.

Сессия будет завершена.

Экспорт данных в CSV

Чтобы выполнить экспорт данных в CSV:

1. На портале администрирования в левом меню выберите раздел **Сессии**.
2. Нажмите кнопку ⋮.
3. Нажмите **[Экспорт CSV]**.
4. Выберите данные для экспорта.
5. Нажмите **[Экспорт]**.

Выбранные данные будут экспортированы в файл CSV-формата.

Глава 8. Политики

8.1. Общие

Только для x2go клиентов (кроме **Доступ к управлению сессиями** и **Балансировка терминальных сессий**).

Политика - это набор настроек для определения поведения системы, применяемый к указанной комбинации пользователей (или группы пользователей) и/или инфраструктурных объектов (групп доставки).

Пользователь с ролью Администратор управляет политиками системы, адаптируя их под текущие потребности других пользователей.

Статусы политик

У каждой политики могут быть следующие статусы.

Таблица 5. Статусы политик

Статус	Описание
Включена	Политика активна и может применяться для определения поведения системы. Политика участвует в моделировании политик
Моделирование,	Политика не активна, не применяется для определения поведения системы, но при этом политика участвует в моделировании политик
Выключена	Политика не применяется для определения поведения системы, а также не участвует в моделировании политик
Черновик	Политика не содержит объекты*, не участвует для определения поведения системы и в моделировании политик. * Политика считается черновиком, если в ней не указаны: • пользовательские объекты(для клиентских политик); • пользовательские и/или инфраструктурные объекты (для сессионных политик); • инфраструктурные объекты (для инфраструктурных политик)

Описание настроек политик

Политика носит разрешающий характер. Она снимает ограничение на

использование соответствующей функции со стороны серверной части, но не переопределяет настройки клиентского приложения. Для фактической работы функции её необходимо также включить в настройках используемого десктоп-клиента.

На вкладке **Общие** раздела **Политики** можно просмотреть,создать и настроить политики.

Termit предлагает выбрать тип создаваемой политики в соответствии с видом настраиваемых параметров: сессионная, клиентская и инфраструктурная.

 Сессионная политика

Сессионная политика применяется в момент открытия сессии и определяет её параметры для указанных пользователей (или групп пользователей) и групп доставки. Изменения не затрагивают уже открытые сессии.

При добавлении политики доступны к выбору следующие настройки:

- **Перенаправление буфера обмена** - Разрешает или запрещает передачу данных с помощью операций вырезания и вставки между сессией и локальным буфером обмена.
- **Перенаправление звука и микрофона** - Разрешает или запрещает приложениям, размещённым на сервере, воспроизводить звуки через звуковое устройство, установленное на ПК, и использовать микрофоны для записи звука.
- **Перенаправление файловой системы (локальных дисков)** - Разрешает или запрещает перенаправление файловой системы от десктоп-клиента и к десктоп-клиенту. Если разрешено, пользователи могут сохранять файлы на свои клиентские диски.
- **Перенаправление смарт-карт** - Разрешает или запрещает перенаправление смарт-карт ПК. Если разрешено, пользователи могут использовать смарт-карты внутри сессии.
- **Доступ к принтерам локального компьютера** - Разрешает или запрещает перенаправление клиентских принтеров на сервер при входе пользователя в сессию.

Базовая сессионная политика - Настройки базовой политики применяются, если они не заданы в более приоритетной включенной политике того же типа.

В базовой сессионной политике всем вышеперечисленным настройкам, кроме «Перенаправление смарт-карт», назначен статус «Разрешено».

 Клиентская политика

Клиентская политика - это набор правил, заданных для конкретного пользователя или группы пользователей, которые определяют поведение и настройки в клиентском

приложении.

При добавлении политики доступны к выбору следующие настройки:

- **Доступ к менеджеру сессий** - Разрешает или запрещает управление сессиями в менеджере сессий. Если разрешено, то пользователи могут закрывать и отключать свои сессии.

Базовая клиентская политика - Настройки базовой политики применяются, если они не заданы в более приоритетной включенной политике того же типа.

В базовой клиентской политике всем вышеперечисленным настройкам назначен статус «Разрешено».

 Инфраструктурная политика

Инфраструктурная политика применяется к конкретным объектам инфраструктуры (группам доставки), которые управляют системными параметрами и поведением на уровне платформы, а не на уровне отдельного пользователя.

При добавлении политики доступны к выбору следующие настройки:

- **Перемещаемые профили: путь к домашнему каталогу** - Позволяет настроить путь к домашнему каталогу для перемещаемых профилей.

Настройка должна быть заполнена, если включена настройка «Перемещаемые профили». Применяется для групп доставки с серверами на ОС Linux

- **Перемещаемые профили** - Включает или выключает использование перемещаемых профилей. Применяется для групп доставки с серверами на ОС Linux.

  Подробнее о настройке перемещаемых профилей в разделе,.

- **Балансировка терминальных сессий** - Составной набор настроек для распределения и оптимизации нагрузки терминальных сессий.

Базовая инфраструктурная политика - Настройки базовой политики применяются, если они не заданы в более приоритетной включенной политике того же типа.

В базовой инфраструктурной политике всем вышеперечисленным настройкам, кроме «Балансировка терминальных сессий: Максимальное количество сессий и Одновременное открытие сессий», назначен статус «Запрещено».

Подробнее о создании политики,.

Описание вкладки «Общие»

На вкладке **Общие** можно:

- Просмотреть общее состояние политик.
- Создать политику.
- Изменить статус политик.
- Посмотреть подробную информацию о политике.
- Изменить приоритет политики.
- Удалить политику.

Состояние политик

На вкладке **Общие** можно просмотреть общее состояние политик, а именно:

- **Общее число политик** - общее число политик, которые созданы в Termit.
- Из них по статусу:
  - **Выключено** - количество политик в статусе «Выключено».
  - **Включено** - количество политик в статусе «Включено».
  - **На моделировании** - количество политик в статусе «Моделирование».
  - **Черновик** - количество политик в статусе «Черновик».

Создание политики

Для создания политики:

1. На портале администрирования, в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. В правом верхнем углу нажмите **[Создать политику]**.
4. Выберите тип политики из списка: **Сессионная**, **Инфраструктурная** или **Клиентская**. Подробнее в разделе.

В зависимости от выбранного типа политики при ее создании:

- на вкладке **Настройки** в окне **Добавление** будут представлены разные наборы настроек на выбор.

- набор доступных вкладок для заполнения в окне добавления определяется типом политики:
  - **Сессионная** — будут доступны вкладки **Пользовательские объекты** и **Объекты инфраструктуры**;
  - **Инфраструктурная** — будет доступна вкладка **Объекты инфраструктуры**;
  - **Клиентская** — будет доступна вкладка **Пользовательские объекты**.

5. На вкладке **Общая информация**:
   - **Политика** — укажите название политики.
   - (Опционально) **Описание** — добавьте описание политики.
6. Нажмите **[Далее]**.
7. На вкладке **Настройки** нажмите ＋.
8. Укажите:
   - **Настройка** — выберите настройку из списка.
   - **Описание** — по умолчанию заполняется описание настройки, выбранной в поле **Настройка**.
   - **Статус** — выберите статус настройки **Разрешено** или **Запрещено**.

1. При выборе в поле **Настройка** значения **Перемещаемые профили: путь к домашнему каталогу** далее доступно к заполнению только поле **Статус**.
2. При выборе в поле **Настройка** значения **Балансировка терминальных сессий** необходимо заполнить настройки балансировки. Подробнее в разделе.

9. Нажмите **Сохранить** › **Далее**.
10. На вкладке **Пользовательские объекты** нажмите ＋.
11. Укажите:
    - **Тип** — выберите тип объекта, на котором будет применена создаваемая политика: **Все**, **Пользователь**, **Группа** или **Каталог**.

Поля **Имя** и **Действие** недоступны для заполнения при выборе в поле **Тип** значения **Все**.

- **Имя** — выберите имя объекта, на котором к которому будет применена создаваемая политика.
- **Действие** — выберите действие политики: **Применять** или **Не применять**

12. Нажмите **Сохранить** › **Далее**.
13. На вкладке **Объекты инфраструктуры** нажмите ＋.
14. Укажите:
    - **Тип группы доставки** — выберите тип объекта, на котором будет применена создаваемая политика: **Все** или **Группа ТС**.

      Поля **Имя** и **Действие** недоступны для заполнения при выборе в поле **Тип** значения **Все**.

    - **Имя** — выберите имя объекта, на котором будет применена создаваемая политика.
    - **Действие** — выберите действие политики: **Применять** или **Не применять**.
15. Нажмите **Сохранить** › **Далее**.
16. На вкладке **Подтверждение информации** проверьте:
    - информацию о политике;
    - настройки политики;
    - объекты инфраструктуры и/или пользователи, к которым будет применена политика.

    При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

17. Нажмите **[Создать]**.

Политика будет сохранена в подразделе, соответствующем её типу, с наименьшим приоритетом. Если в политике указаны объекты инфраструктуры/пользователи, то она перейдет в статус **Моделирование**. Если нет - то перейдет в статус **Черновик**.

Статус **Черновик** новой политике присваивается в случае:

- если в клиентской политике не указаны пользовательские объекты;
- если в сессионной политике на указаны пользовательские и/или инфраструктурные объекты;
- если в инфраструктурной политике не указаны инфраструктурные объекты.

Из статуса «Черновик» возможен переход только в статус «Моделирование».

После создания политики можно:

- Перевести политику в статус «Включена».
- Запустить процесс моделирования на вкладке **Моделирование** (если политика в статусе «Черновик»).
- Изменить политику.
- Включить и выключить политику (если политика не в статусе «Черновик»).
- Удалить политику.

Балансировка терминальных сессий

Чтобы определить, к какому серверу будет подключен пользователь, используется следующая формула:

Индекс балансировки сервера= **Максимальный индекс метрики** + **(Сумма остальных индексов метрики /(Количество активных метрик -1))** × 0.05

Где:

- Максимальный индекс метрики = максимальное значение индекса из активных метрик.
- Сумма остальных индексов метрики = сумма оставшихся активных метрик (за вычетом максимальной).
- (Количество активных метрик -1) - количество метрик, разрешенных в политике балансировки, за вычетом максимальной.

Выбирается сервер с наименьшим индексом в группе.

Чтобы настроить балансировку:

1. На портале администрирования в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. В правом верхнем углу нажмите **[Создать политику]**.
4. Выберите тип политики из списка блоке **Инфраструктурные**.
5. На вкладке **Общая информация**:
   - **Политика** — укажите название политики.
   - (Опционально) **Описание** — добавьте описание политики.
6. Нажмите **[Далее]**.
7. На вкладке **Настройки** нажмите ＋.
8. Укажите:

- **Настройка** — выберите настройку из списка.
- Задайте статус и предел метрики. Значение не может быть отрицательным:
  - *Одновременное открытие сессий* - Ограничивает количество сессий, которые могут открываться одновременно. При превышении этого лимита сервер временно исключается из балансировки нагрузки. Указывается в количестве сессий.
  - *Загрузка ЦП* - Включает загрузку ЦП для балансировки. При превышении указанного значения сервер исключается из балансировки нагрузки. Значение указывается в процентах.
  - *Длина очереди диска* - Включает длину очереди диска для балансировки. При превышении указанного значения сервер исключается из балансировки нагрузки. Значение указывается в количестве операций в очереди.
  - *Максимальное количество сессий* - Включает максимальное количество сессий для балансировки. При превышении указанного значения сервер исключается из балансировки нагрузки. Значение указывается в количестве сессий.Если все параметры балансировки выключены, балансировка будет осуществляться по этому параметру со значением 250.
  - *Загрузка ОЗУ* - Включает загрузку ОЗУ для балансировки. При превышении указанного значения сервер исключается из балансировки нагрузки. Значение указывается в процентах. Параметр учитывает «Базовый объем ОЗУ».
  - *Базовый объем ОЗУ* - Включает загрузку ОЗУ для балансировки. При превышении указанного значения сервер исключается из балансировки нагрузки. Значение указывается в процентах. Параметр учитывает «Базовый объем ОЗУ».

9. Нажмите **Сохранить** › **Далее**.
10. На вкладке **Объекты инфраструктуры** нажмите ＋.
11. Укажите:
    - **Тип группы доставки** — выберите тип объекта, на котором будет применена создаваемая политика: **Все** или **Группа ТС**.

      Поля **Имя** и **Действие** недоступны для заполнения при выборе в поле **Тип** значения **Все**.

    - **Имя** — выберите имя объекта, на котором будет применена создаваемая политика.
    - **Действие** — выберите действие политики: **Применять** или **Не применять**
12. Нажмите **Сохранить** › **Далее**.

13. На вкладке **Подтверждение информации** проверьте:
    - информацию о политике;
    - настройки политики;
    - объекты инфраструктуры и/или пользователи, к которым будет применена политика.

    При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

14. Нажмите **[Создать]**.
15. На вкладке **Подтверждение** проверьте информацию о политике и нажмите **[Сохранить]**.

Балансировка нагрузки серверов будет настроена.

Включение политики

Чтобы включить политику:

1. В левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. Наведите курсор на нужную политику и нажмите ⊳.

После этого настроенные правила будут применяться на пользователей/объекты инфраструктуры и статус политики изменится на «Включена».

Выключение политики

Чтобы выключить политику:

1. В левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. Наведите курсор на нужную политику и нажмите ⊙.

После этого настроенные правила не будут применяться на пользователей/объекты инфраструктуры и статус политики изменится на «Выключена».

Перевод политики в статус «Моделирование»

Для удобства подготовки политики к работе предусмотрен процесс моделирования для политики.

В статусе моделирования выбранная политика не влияет на работу Termit, а предоставляет возможность пользователю просмотреть модель её работы с помощью средств моделирования без необходимости её фактического применения.

Для перевода политики в статус «Моделирование»:

1. На портале администрирования, в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. Наведите курсор на нужную политику и нажмите .
4. Нажмите **[Да]**.

Статус политики будет изменен на «Моделирование».

После изменения статуса политики на «Моделирование» пользователь сможет просмотреть на модель политики без фактического ее применения на вкладке **Моделирование**,.

Изменение приоритета политики

Каждая созданная политика имеет свой уникальный порядок в рамках типа политики (сессионной, клиентской, инфраструктурной). Приоритет политики определяет какая из одинаковых настроек, заданных в разных включенных политиках, будет действовать на пользовательские/инфраструктурные объекты. При построении итоговой политики из числа соответствующих сессии пользователя, настройки этих политик объединяются.

При создании политика получает наименьший приоритет из списка в рамках одного типа.

Для изменения приоритета политики:

1. На портале администрирования, в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. В правом верхнем углу нажмите **[Изменить приоритет]**.
4. Переместите политику на необходимый приоритет:
   - В столбце приоритет:
     - Слева отображается исходный приоритет.
     - Справа отображается направление изменения приоритета политики.
5. Нажмите **[Сохранить]**.

После сохранения у политики будет изменен порядковый номер и приоритет ее действия.

Изменение политики

Базовые сессионные, клиентские и инфраструктурные политики изменить нельзя.

Чтобы изменить политику:

1. На портале администрирования, в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.
3. Наведите курсор на политику и нажмите ✎.
4. Измените параметры:
5. На вкладке **Общая информация**:
   - **Политика** — название политики.
   - (Опционально) **Описание** — описание политики.
6. Нажмите **[Далее]**.
7. На вкладке **Настройки** измените настройки политики. Для этого наведите курсор на нужную политику и нажмите ✎.

   Чтобы добавить новую настройку политики, нажмите +. Подробнее о настройке.

   Для удаления настройки наведите курсор на нужную политику и нажмите 🗑. Подтвердите действие, нажав **[Да]**.

8. Нажмите **Сохранить** › **Далее**.
9. (Опционально, если тип политики **Клиентская** и **Сессионная**) На вкладке **Пользовательские объекты** нажмите +.
10. Укажите:
    - **Тип** — выберите тип объекта, на котором будет применена создаваемая политика: **Все**, **Пользователь**, **Группа** или **Каталог**.

      Поля **Имя** и **Действие** недоступны для заполнения при выборе в поле **Тип** значения **Все**.

    - **Имя** — выберите имя объекта, на котором будет применена создаваемая политика.
    - **Действие** — выберите действие политики: **Применять** или **Не применять**

Для удаления пользователя/группы пользователей наведите курсор на нужную группу пользователей/пользователя и нажмите 🗑. Подтвердите действие, нажав **[Да]**.

11. Нажмите **Сохранить** › **Далее**.
12. (Опционально, если тип политики **Инфраструктурная** и **Сессионная**) На вкладке **Объекты инфраструктуры** нажмите ＋.
13. Укажите:
    - **Тип** — выберите тип объекта, на котором будет применена создаваемая политика: **Все** или **Группа ТС**.

      Поля **Имя** и **Действие** недоступны для заполнения при выборе в поле **Тип** значения **Все**.

    - **Имя** — выберите имя объекта, на котором будет применена создаваемая политика.
    - **Действие** — выберите действие политики: **Применять** или **Не применять**
14. Нажмите Нажмите **[Далее]**.

Для удаления объекта инфраструктуры наведите курсор на нужную группу и нажмите 🗑. Подтвердите действие, нажав **[Да]**.

15. Нажмите **[Далее]**.
16. На вкладке **Подтверждение** проверьте:
    - информацию о политике;
    - настройки политики;
    - объекты инфраструктуры и/или пользователи, на которые будет применена политика.

      При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

17. Нажмите **[Сохранить]**.

Политика будет изменена.

Удаление политики

Чтобы удалить политику:

1. На портале администрирования, в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Общие**.

3. Наведите курсор на политику и нажмите .
4. Нажмите **[Да]**.

Политика будет удалена.

8.2. Моделирование

Для удобства подготовки политики к работе предусмотрен процесс моделирования для каждой политики.

Моделирование — это процесс проверки, анализа и прогнозирования того, как настройки из политик будут применяться к выбранным объектам инфраструктуры (пользователям, серверам, группам и т.д.).

Моделирование позволяет администратору:

- Оценить эффект настроек до их применения в продуктивной среде.
- Выявить конфликты между политиками (например, когда одна политика разрешает доступ, а другая запрещает).
- Проверить корректность назначения политик конкретным объектам.

В процессе моделирования учитываются только те политики (или отдельные настройки внутри политик), которые находятся в статусе «Моделирование». Это означает, что такие настройки ещё не активны и не влияют на реальную работу системы — они лишь участвуют в расчёте прогноза.

Результат моделирования показывает, какие именно настройки и из каких политик будут применены к заданным объектам, если перевести эти политики в активный статус. Таким образом, администратор может безопасно тестировать изменения и принимать взвешенные решения перед их включением.

На вкладке **Моделирование** можно:

- Найти необходимый отчет о моделировании по дате и времени, нажав .
- Обновить список моделирований, нажав .
- Просмотреть отчет о моделировании, нажав .
- Обновить моделирование, наведя курсор на необходимое моделирование и нажав .

В списке сохраняется не более 100 записей.

Создание моделирования

Для создания моделирования:

1. На портале администрирования в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Моделирование**.
3. Нажмите на кнопку **[Создать моделирование]**.
4. В поле **Тип политики** выберите значение **Сессионная**, **Инфраструктурная**, **Клиентская** или **Все**.

В зависимости от выбранного типа настройки:

- **Сессионная** будут доступен для заполнения блок **Пользовательские объекты** и **Объекты инфраструктуры**;
- **Инфраструктурная** будет доступен для заполнения блок **Объекты инфраструктуры**;
- **Клиентская** будут доступна для заполнения вкладка **Пользовательские объекты**;
- **Все** будут доступна для заполнения вкладка **Пользовательские объекты** и **Объекты инфраструктуры**.

5. В блоке **Пользовательские объекты** выберите значение **Все**, **Каталог**, **Пользователь** или **Группа пользователей**.

   При выборе значения **Все**, **Каталог**, **Пользователь** или **Группа пользователей** выберите каталог, пользователя или группу пользователей, на которые необходимо создать моделирование.

6. В блоке **Объекты инфраструктуры** выберите значение **Все** или **Группы ТС**.

   При выборе значения **Группы ТС** выберите группу ТС, на которую необходимо создать моделирование.

7. Нажмите **[Создать]**.

Новое моделирование появится в списке моделирований.

Проведение повторного моделирования

Для проведения повторного моделирования:

1. На портале администрирования в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Моделирование**.
3. Наведите курсор на необходимое моделирование и нажмите .
4. Нажмите **[Да]**.

Будет проведено повторное моделирование политики.

Просмотр отчета о моделировании

Для просмотра отчета о моделировании:

1. На портале администрирования в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Моделирование**.
3. Наведите курсор на необходимое моделирование и нажмите .
4. Просмотрите отчет о моделировании и нажмите **[Закрыть]**.

   При необходимости можно повторить моделирование.

Удаление моделирования

Для того, чтобы удалить моделирование:

1. На портале администрирования в левом меню выберите раздел **Политики**.
2. Перейдите на вкладку **Моделирование**.
3. Наведите курсор на необходимое моделирование и нажмите .
4. Нажмите **[Да]**.

   Моделирование будет удалено. Также оно будет отсутствовать в списке.

Глава 9. Настройки

9.1. Общие настройки

Раздел содержит инструкции по настройке системы Termit.

HTTPS

Чтобы изменить адрес портала внутреннего доступа, загрузить ключ, сертификат и цепочку сертификатов:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **HTTPS** и нажмите ✎.
2. При необходимости измените адрес портала внутреннего доступа.
3. Чтобы загрузить сертификат или цепочку сертификатов, нажмите на поле **Сертификат**.
4. Чтобы загрузить закрытый ключ, нажмите на поле **Закрытый ключ**.
5. Укажите доверенные IP-адреса и подсети балансировщиков в поле **Разрешенные IP-адреса балансировщика**. Заголовки `X-SSL-Client-Cert` и `X-Real-IP`, пришедшие не из этого перечня, брокер игнорирует.
6. Нажмите **[Сохранить]**.

Настройки будут сохранены.

Подробнее о генерации самоподписанного сертификата,.

Внешний вид десктоп-клиента

Чтобы список опубликованных приложений и рабочих столов в десктоп-клиенте был разделен, настройте внешний вид в десктоп-клиенте:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Внешний вид десктоп-клиента** и нажмите ✎.
2. Активируйте опцию **Разделение объектов на приложения и рабочие столы**.
3. Нажмите **[Сохранить]**.

Приложения и рабочие столы будут разделены по типу в десктоп-клиенте.

Аутентификация

Чтобы настроить аутентификацию:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Аутентификация** и нажмите ✎.
2. Активируйте опции:
   - **Аутентификация по логину и паролю** — опция включена по умолчанию. Если её отключить, вход в систему будет возможен только через альтернативные методы аутентификации (через Kerberos или смарт-карту). Исключение — учетная запись локального администратора.
   - **Смена пароля пользователем** — активируйте опцию, если необходимо разрешить пользователю смену пароля.

   > Поле **Смена пароля пользователем** доступно к изменению при включенной опции в поле **Аутентификация по логину и паролю**.

3. Нажмите **[Сохранить]**.

Настройки будут сохранены.

Многофакторная аутентификация

> При включенной опции **Аутентификация по логину и паролю** в разделе **Аутентификация** настройки МФА для входа по логину и паролю не применяются. Чтобы отключить опцию, перейдите в раздел.

Чтобы настроить многофакторную аутентификацию (МФА):

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Многофакторная аутентификация** и нажмите ✎.
2. В поле **Внутренние пользователи** активируйте опции:
   - **Многофакторная аутентификация при использовании Kerberos**, если для аутентификации внутренних пользователей на портале администрирования, в десктоп-клиенте и на пользовательском портале по Kerberos нужно использовать МФА.
   - **Многофакторная аутентификация при использовании логина и пароля**, если для аутентификации внутренних пользователей на портале администрирования, в десктоп-клиенте и на пользовательском портале по имени и паролю нужно использовать МФА.

3. В поле **Внешние пользователи** активируйте опцию **Многофакторная аутентификация при использовании логина и пароля**, если для аутентификации внешних пользователей в десктоп-клиенте и на пользовательском портале по имени и паролю нужно использовать МФА.
4. В поле **Порядок ОТП** активируйте опцию **Запрашивать ОТП до пароля при использовании МФА**, если необходимо запросить одноразовый пароль до ввода данных (логина и пароля). Правило действует глобально для внутренних и внешних пользователей.

- Настройка доступна, если активна опция **Многофакторная аутентификация при использовании логина и пароля**.
- Поле **Запрашивать ОТП до пароля при использовании МФА** работает корректно только при использовании логина и пароля в качестве первого фактора аутентификации.

5. В блоке **Исключения МФА** укажите LDAP-группы, пользователи которых проходят аутентификацию без использования МФА. Правило действует глобально для внешних и внутренних пользователей.
6. Нажмите **[Сохранить]**.

Многофакторная аутентификация будет настроена.

Далее настройте RADIUS-сервер.

Пользовательский портал

Можно включить возможность подключения пользователей через браузер без установки десктоп-клиента.

Чтобы включить возможность подключения пользователей через браузер:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Пользовательский портал** и нажмите ✎.
2. Активируйте опцию **Доступ к пользовательскому порталу**.
3. Нажмите **[Сохранить]**.

Доступ к пользовательскому порталу через браузер будет включен.

1. При включённом доступе к пользовательскому порталу для открытия административного вида портала необходимо добавить к адресу /admin. Пример: https://broker.example.com/admin.
2. При подключении к приложениям/рабочим столам через пользовательский портал используется протокол «WebSocket». Некоторые сетевые устройства требуют дополнительной настройки для поддержки этого протокола.

Syslog/SIEM

Можно настроить переадресацию журнала в syslog-сервер.

Сведения о каждом событии в Termit отправляются как отдельное syslog-сообщение. Текст syslog-сообщения соответствует информации о событии, отображающейся в веб-интерфейсе системы в разделе Журнал событий.

Чтобы настроить параметры для интеграции Syslog:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Syslog/SIEM** и нажмите ✎.
2. Активируйте опцию **Использование**, чтобы запись событий отправлялась на syslog-сервер.
3. При включенной интеграции в параметрах:
   - **Адрес сервера** — укажите адрес сервера.
   - **Порт** — укажите порт. По умолчанию 514 (6514 для TLS).
   - **Протокол** — выберите UDP или TCP.
   - **Формат сообщений** — выберите спецификацию RFC3164 или RFC5424.
   - **Код подсистемы** (facility) — выберите local0-local7.
   - **TLS для отправки логов в Syslog** — выберите **Выключено** или **Включено**. При выборе протокола TLS следует использовать доверенные сертификаты, указанные администратором в соответствующем разделе.
4. Нажмите **[Сохранить]**.

Параметры для интеграции Syslog будут настроены.

Доверенные сертификаты

Доверенные сертификаты применяются для проверки соединения с LDAP-каталогами по

протоколам LDAP StartTLS и LDAP over SSL. Кроме того, доверенные сертификаты необходимы для Syslog, когда он использует TLS для отправки логов.

Чтобы добавить доверенный сертификат:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Доверенные сертификаты** и нажмите ✎.
2. Чтобы добавить сертификат, нажмите + и загрузите его. Поддерживаются форматы PKCS#12/PEM/CER/CRT (в кодировке Base-64).

Если цепочка доверенных сертификатов представлена в одном файле формата PEM, её необходимо разбить на отдельные части и загружать каждый сертификат в виде отдельного файла. При загрузке цепочки одним файлом в интерфейсе будет отображаться только подчинённый сертификат.

3. При необходимости активируйте опцию **Задать пароль** и задайте пароль для сертификата.
4. Нажмите **[Сохранить]**.

Добавленный сертификат появится в списке.

Чтобы удалить:

1. Наведите курсор на сертификат и нажмите ⋮.
2. Нажмите **[Удалить сертификат]**.
3. Нажмите **[Да]**.

Сертификат будет удален.

Администратор системы

«tadm» — локальная учетная запись, которая предназначена только для настроек брокера. Ее нельзя использовать для входа в десктоп-клиент, запуска приложений и рабочих столов.

«admin» — пароль по умолчанию от локальной учетной записи.

Обязательно измените пароль для повышения уровня безопасности системы.

Изменение параметров администратора системы

Чтобы изменить параметры администратора системы:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Администратор системы** и нажмите .
2. При необходимости измените имя локального администратора системы.
3. Введите старый пароль и задайте новый.
4. Подтвердите новый пароль.
5. Нажмите **[Сохранить]**.

Данные об администраторе системы будут изменены.

Разблокировка учетной записи администратора системы

При неудачной авторизации в систему Termit учетная запись блокируется. Подробнее смотрите в разделе Политика блокировки встроенных учетных записей.

Для разблокировки учетной записи администратора системы на портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Администратор системы** и нажмите на . Учетная запись будет разблокирована.

Глубина хранения журналов событий

В системе можно очищать старые записи журнала событий.

Чтобы настроить срок хранения записей:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Глубина хранения журнала событий** и нажмите .
2. При включенной опции **Никогда не удалять** старые записи в журнале событий не будут очищаться.

   Чтобы задать свой срок хранения, отключите эту опцию и выберите значение:

   - **Срок хранения событий (дней)** — период хранения событий журнала;
   - **Время запуска** — время запуска очистки журнала событий.

3. Нажмите **[Сохранить]**.

После очистки в журнале событий появится запись о статусе операции: сколько событий было удалено, дата самой старой и самой новой сессии.

Чтобы настроить ограничение журнала событий по объёму выделенной памяти, выполните настройки через REST API. Подробнее о настройке.

Глубина хранения сессий

В системе можно очищать историю закрытых сессий пользователей.

Чтобы настроить срок хранения:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Глубина хранения сессий** и нажмите ✎.
2. При включенной опции **Никогда не удалять** старые записи в журнале событий не будут очищаться.

   Чтобы задать свой срок хранения, отключите эту опцию и задайте:

   - **Срок хранения сессий (дней)** — период хранения истории закрытых сессий;
   - **Время запуска** — время запуска очистки истории закрытых сессий.
3. Нажмите **[Сохранить]**.

После очистки в журнале событий появится запись о статусе операции: сколько сессий было удалено, дата самой старой и новой сессии.

RADIUS

RADIUS-сервер (Remote Authentication Dial-In User Service) — сервер для централизованной аутентификации, авторизации и учета (AAA) пользователей.

Чтобы настроить RADIUS-сервер для аутентификации:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **RADIUS** и нажмите ✎.
2. Чтобы использовать RADIUS-сервер, активируйте опцию **Использование**.
3. При включенной опции в параметрах задайте:

- **Адрес сервера** — IP-адрес RADIUS-сервера.
- **Порт** — по умолчанию порт 1812. Вы можете указать другой.
- **Секрет для подключения к RADIUS-серверу** — общий пароль между RADIUS-клиентом и RADIUS-сервером.

Проверьте, что все брокеры добавлены в конфигурацию RADIUS-сервера в качестве RADIUS-клиентов.

- **Идентификатор NAS для внутренних пользователей** — символы NAS ID для внутренних пользователей.
- **Идентификатор NAS для внешних пользователей** — символы NAS ID для внешних пользователей.

При подключении десктоп-клиента RADIUS-сервер использует NAS ID (Network Access Server Identifier) для:

- классификации запросов, которые поступили от RADIUS-клиентов;
- применения соответствующих настроек или политик для внутренних и внешних пользователей.

- **Таймаут подключения (сек.)** — время ожидания отклика от RADIUS-сервера при попытке установить с ним соединение.
- **Количество попыток подключения** — количество попыток подключения к RADIUS-серверу.

4. Активируйте опцию **Использование RADIUS только для проверки второго фактора**, если требуется использовать RADIUS-сервер только для проверки второго фактора (например, TOTP). В этом случае проверка первого фактора будет выполняться брокером через LDAP-сервер.

Режим проверки факторов должен быть одинаковым в Termit и на RADIUS-сервере.

Настройка **Использование RADIUS только для проверки второго фактора** в Termit должна соответствовать параметру **first-factor-authentication-source** в конфигурационном файле клиента на RADIUS-сервере (например, **/opt/multifactor/radius/clients/<имя_клиента>.config**):

- опция включена — установите значение **none** (RADIUS проверяет только второй фактор);
- опция выключена — установите значение **ldap** (RADIUS проверяет оба фактора).

5. В параметре **Протокол аутентификации RADIUS** выберите протокол **PAP**, **CHAP** или **MSCHAPv2**.
6. Нажмите **[Сохранить]**.

RADIUS-сервер будет настроен.

Политика блокировки встроенных учетных записей

Политика блокировки встроенных учетных записей необходима для обеспечения безопасности системы и применяется только для локальной учетной записи «tadm». Учетная запись блокируется, если пользователь совершает несколько неудачных попыток входа в систему Termit. Это помогает предотвратить несанкционированный доступ к данным и ресурсам компании.

По умолчанию политика включена, и после трех неудачных попыток входа в систему учетная запись блокируется на один час.

Чтобы задать собственную политику блокировки встроенных учетных записей:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки**, наведите курсор на **Политика блокировки встроенных учетных записей** и нажмите ✎.
2. Включите опцию **Использование**, если хотите, чтобы политика блокировки работала. Или вы можете отключить эту опцию, если не хотите применять политику блокировки.
3. При включенной опции в параметрах задайте:
   - **Число неудачных попыток входа** — число неудачных попыток, после которых учетная запись пользователя будет заблокирована.
   - **Срок блокировки учетных записей (мин)** — срок блокировки учетных записей.

     Во время блокировки учетной записи попытки входа невозможны, что предотвращает подбор пароля методом перебора или с использованием вредоносного ПО. А пользователь, который действительно хочет войти в свой аккаунт, за это время может восстановить доступ, если он забыл пароль или столкнулся с временными техническими проблемами.

4. Нажмите **[Сохранить]**.

Политика блокировки встроенных учетных записей будет задана.

Инструкция по разблокировке учетной записи администратора системы приведена в разделе Разблокировка учетной записи администратора системы.

Токены

В Termit есть возможность настройки времени жизни токенов.

Чтобы задать значения токенов:

1. На портале администрирования в разделе **Настройки**, на вкладке **Общие настройки**, наведите курсор на **Токены** и нажмите ✎.
2. Задайте значения параметров в соответствующих полях:
   - **Время жизни access-токена** — определяет период, в течение которого токен остаётся действительным после выдачи. По истечении этого срока для продолжения работы потребуется повторная аутентификация. Укажите значение в формате **"дд.чч.мм"**.
   - **Время жизни refresh-токена** — определяет период, в течение которого refresh-токен может быть использован для получения новой пары токенов (access и refresh) после истечения срока действия access-токена. По окончании этого срока пользователю потребуется выполнить повторную аутентификацию. Укажите значение в формате **"дд.чч.мм"**.
   - **Время простоя** — определяет максимальный период бездействия пользователя, после которого сессия автоматически завершается. При наличии активности в течение этого времени сессия остаётся активной. Укажите значение в формате **"дд.чч.мм"**.
   - **Время жизни после аутентификации** — определяет максимальный период существования сессии с момента успешного входа пользователя. По истечении этого времени сессия завершается независимо от наличия активности. Укажите значение в формате **"дд.чч.мм"**.
3. Нажмите **[Сохранить]**.

   Значения времени жизни токенов будут настроены.

   Чтобы сбросить все введенные ранее значения - нажмите **Сбросить › Да**.

9.2. LDAP-каталоги

LDAP (Lightweight Directory Access Protocol) — протокол, который используется для получения информации из служб каталогов (AD, FreeIPA, ALD Pro, SambaDC, Red ADM и так далее) о пользователях, группах и связях между ними. Эта информация в дальнейшем используется для аутентификации и авторизации пользователей на портале администрирования, в десктоп-клиенте и на ТС.

LDAP представляет информацию об этих сущностях в виде набора объектов (пользователь, группа), каждый из которых имеет определенный набор атрибутов (имя пользователя, имя группы, список членов группы, номер телефона пользователя). Можно добавить несколько групп. Также поддерживаются вложенные группы.

Для работы пользователей с Termit необходимо, чтобы система могла выполнять поиск пользователей в LDAP-каталоге, получать список групп, в которые входит пользователь, и т.д. Для этого администратору нужно указать имена классов и ряд атрибутов для объектов «Пользователь» и «Группа»:

- Общие атрибуты для классов объектов:
  - **Атрибут для идентификации объектов** — в значении этого атрибута хранится уникальный ID объекта.
  - **Атрибут, содержащий имя объекта, указанное для списка членов групп** — в значении этого атрибута описано уникальное имя объекта в списке членов групп. Имя объекта однозначно определяет его положение в иерархической структуре каталога.
- Атрибуты для класса объекта «Пользователь»:
  - **Атрибут для получения отображаемого имени пользователя** — значение этого атрибута применяется при отображении пользователей в интерфейсе, например, при входе в систему.
  - **Атрибут для поиска пользователя** — атрибут применяется для поиска пользователя по его имени при аутентификации на портале администрирования или в десктоп-клиенте.
  - **Атрибут для аутентификации на терминальном сервере Linux** — в значении этого атрибута описано имя, которое будет передаваться на сервер под управлением Linux.
  - **Атрибут для аутентификации на терминальном сервере Windows** — в значении этого атрибута описано имя, которое будет передаваться на сервер под управлением Windows.
- Атрибуты для класса объекта «Группа»:

- **Атрибут для получения отображаемого имени группы** — значение этого атрибута применяется при отображении групп в интерфейсе. Например, при добавлении ролей или при настройке прав на запуск приложения.
- **Атрибут со списком членов групп** — в значении этого атрибута находится информация о группе, в состав которой входят пользователи и другие группы.

В Termit поддерживаются:

- следующие LDAP-каталоги для аутентификации пользователей по паролю и получения информации о пользователях, группах и связях между ними:
  - AD
  - SambaDC
  - Red ADM
  - FreeIPA
  - ALD Pro
  - OpenLDAP
- защищенные протоколы передачи данных LDAP Over SSL и LDAP StartTLS.

На вкладке **LDAP-каталоги** при наведении курсора на полное имя каталога можно:

- проверить соединение, нажав ;
- удалить LDAP-каталог, нажав ;
- синхронизировать данные LDAP-каталога, нажав . Можно запустить полную или инкрементальную синхронизацию;
- настроить Kerberos, нажав .
- изменить настройки LDAP-каталога, нажав .

Добавление LDAP-каталога

Чтобы добавить LDAP-каталог:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и нажмите **[Добавить каталог]**.
3. Задайте параметры для подключения службы каталогов:
   - **Полное имя** — отображаемое имя в списке LDAP-каталогов и при входе в систему.
   - **Базовое уникальное имя**. Например, для домена example.com: «DC=example,DC=com».

- **Имя пользователя**. Например, для домена example.com: «CN=termitsvc,CN=users,DC=example,DC=com».
- **Пароль** — пароль от сервисной учетной записи.

4. Нажмите **[Далее]**.
5. Чтобы задать атрибуты используемого LDAP-каталога, укажите:
   - **Тип LDAP-каталога** — тип: **AD**, **SambaDC**, **FreeIPA** или **Другой**.

Тип зависит от выбранной схемы LDAP:

- Для Red ADM требуется выбрать тип каталога **AD**.
- Для Samba DC требуется выбрать тип каталога **AD** и вручную указать для параметра **Атрибут для аутентификации на терминальном сервере Windows** значение userPrincipalName.
- Для ALD Pro требуется выбрать тип каталога **FreeIPA**.
- Для OpenLDAP и других реализаций LDAP-каталогов требуется выбрать тип **Другой**.

AD

- **Класс объекта «Пользователь»** — user
- **Класс объекта «Группа»** — group
- **Атрибут для идентификации объектов** — objectGUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — samAccountName
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — distinguishedName
- **Атрибут для аутентификации на терминальном сервере Linux** — samAccountName
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — uSNChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

Samba DC

Использование шаблона Samba DC поддерживается начиная с версии **2.5.1**. В версии **2.5.0** данный шаблон недоступен. Вместо этого воспользуйтесь шаблоном **AD**, заменив вручную параметр **Атрибут для аутентификации на терминальном сервере Windows** значением userPrincipalName.

- **Класс объекта «Пользователь»** — user
- **Класс объекта «Группа»** — group
- **Атрибут для идентификации объектов** — objectGUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — samAccountName
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — distinguishedName
- **Атрибут для аутентификации на терминальном сервере Linux** — samAccountName
- **Атрибут для аутентификации на терминальном сервере Windows** — userPrincipalName
- **Атрибут для поиска только измененных объектов** — uSNChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

При подключении Samba DC к брокеру рекомендуется использовать только защищённые протоколы **LDAP over SSL** или **LDAP StartTLS**

FreeIPA

- **Класс объекта «Пользователь»** — inetuser
- **Класс объекта «Группа»** — ipausergroup
- **Атрибут для идентификации объектов** — ipaUniqueID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — uid
- **Атрибут со списком членов групп** — member

- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — dn
- **Атрибут для аутентификации на терминальном сервере Linux** — uid
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — whenChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

Другой (для OpenLDAP)

- **Класс объекта «Пользователь»** — posixAccount
- **Класс объекта «Группа»** — posixGroup
- **Атрибут для идентификации объектов** — entryUUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — uid
- **Атрибут со списком членов групп** — memberUid
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — uid
- **Атрибут для аутентификации на терминальном сервере Linux** — uid
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — modifyTimestamp
- Выключите опцию **Поддержка range для получения членов группы**.

6. Нажмите **[Далее]**.
7. На вкладке **Синхронизация**, укажите:
   - **Период синхронизации (мин.)**.
   - Включите опцию **Инкрементальная синхронизация** для включения частичной синхронизации.

1. Опция **Инкрементальная синхронизация** и поле **Период инкрементальной синхронизации (мин.)** доступны только для LDAP-каталогов с типом **AD**.
2. Значение должно быть меньше периода полной синхронизации.

   - **Период инкрементальной синхронизации (мин.)**

8. Нажмите **[Далее]**.
9. На вкладке **Список серверов** добавьте LDAP-серверы. Чтобы добавить адрес сервера LDAP, нажмите ＋.

Система всегда работает с первым LDAP-сервером. Если сервер становится недоступен, система переходит к следующему.

10. Укажите:
    - **Адрес сервера** — IP-адрес или FQDN LDAP-сервера, например «termit-example-01.com».
    - **Протокол** — выберите из списка:

Перед выбором протоколов LDAP Over SSL и LDAP StartTLS добавьте доверенный сертификат,.

      - **LDAP** — технология шифрования данных при подключении к LDAP-серверу не используется. Данные передаются в открытом виде по порту 389. Не рекомендуется использовать в продуктовых инсталляциях.
      - **LDAP Over SSL** — защищенная версия протокола LDAP, которая использует технологию шифрования SSL/TLS при подключении к LDAP-серверу по порту 636.
      - **LDAP StartTLS** — защищенная версия протокола LDAP, при использовании которой сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование.
    - **Порт** — порт выбирается автоматически в зависимости от выбранного протокола. При необходимости параметр можно изменить.
11. Нажмите **Сохранить › Далее**.
12. На вкладке **Подтверждение информации** проверьте:
    - заданные на предыдущих шагах параметры;
    - соединение. При успешном соединении появится сообщение «Проверка соединения прошла успешна».

    При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.
13. Нажмите **[Сохранить]**.

Будет добавлен LDAP-каталог с заданными параметрами.

Для синхронизации данных созданного LDAP-каталога нажмите ⟳. Состояние синхронизации LDAP и системы смотрите в разделе Журнал событий.

При использовании более одной службы каталогов каждый из каталогов должен быть добавлен на портале администрирования в раздел **Настройки › LDAP-каталоги**. Поддерживаемые типы доверительных отношений смотреть в разделе,.

Изменение настроек LDAP-каталога

Чтобы изменить настройки LDAP-каталога:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и наведите курсор на полное имя каталога.
3. Нажмите ✎.
4. Активируйте/деактивируйте опцию **LDAP используется**, если необходимо включить/отключить LDAP-каталог.
5. При включенном LDAP измените параметры:
   - **Полное имя** — отображаемое имя в списке LDAP-каталогов и при входе в систему.
   - **Базовое уникальное имя**. Например, для домена example.com: «DC=example,DC=com».
   - **Имя пользователя**. Например, для домена example.com: «CN=termitsvc,CN=users,DC=example,DC=com».
   - (Опционально) **Пароль** — пароль от сервисной учетной записи.
6. Нажмите **[Далее]**.
7. Чтобы задать атрибуты используемого LDAP-каталога, укажите:
   - **Тип LDAP-каталога** — тип: **AD**, **FreeIPA** или **Другой**.

Тип зависит от выбранной схемы LDAP:

- Для Red ADM требуется выбрать тип каталога **AD**.
- Для Samba DC требуется выбрать тип каталога **AD** и вручную указать для параметра **Атрибут для аутентификации на терминальном сервере Windows** значение userPrincipalName.
- Для ALD Pro требуется выбрать тип каталога **FreeIPA**.
- Для OpenLDAP и других реализаций LDAP-каталогов требуется выбрать тип **Другой**.

AD

- **Класс объекта «Пользователь»** — user
- **Класс объекта «Группа»** — group
- **Атрибут для идентификации объектов** — objectGUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — samAccountName
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — distinguishedName
- **Атрибут для аутентификации на терминальном сервере Linux** — samAccountName
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — uSNChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

SambaDC

Использование шаблона Samba DC поддерживается начиная с версии **2.5.1**. В версии **2.5.0** данный шаблон недоступен. Вместо этого воспользуйтесь шаблоном **AD**, заменив вручную параметр **Атрибут для аутентификации на терминальном сервере Windows** значением userPrincipalName.

- **Класс объекта «Пользователь»** — user
- **Класс объекта «Группа»** — group
- **Атрибут для идентификации объектов** — objectGUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — samAccountName
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — distinguishedName

- **Атрибут для аутентификации на терминальном сервере Linux** — samAccountName
- **Атрибут для аутентификации на терминальном сервере Windows** — userPrincipalName
- **Атрибут для поиска только измененных объектов** — uSNChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

При подключении Samba DC к брокеру рекомендуется использовать только защищённые протоколы **LDAP over SSL** или **LDAP StartTLS**

FreeIPA

- **Класс объекта «Пользователь»** — inetuser
- **Класс объекта «Группа»** — ipausergroup
- **Атрибут для идентификации объектов** — ipaUniqueID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — uid
- **Атрибут со списком членов групп** — member
- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — dn
- **Атрибут для аутентификации на терминальном сервере Linux** — uid
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — whenChanged
- Для чтения большого количества пользователей в группе включите опцию **Поддержка range для получения членов группы**.

Другой (для OpenLDAP)

- **Класс объекта «Пользователь»** — posixAccount
- **Класс объекта «Группа»** — posixGroup
- **Атрибут для идентификации объектов** — entryUUID
- **Атрибут для получения отображаемого имени пользователя** — cn
- **Атрибут для получения отображаемого имени группы** — cn
- **Атрибут для поиска пользователя** — uid
- **Атрибут со списком членов групп** — memberUid

- **Атрибут, содержащий имя объекта, указанное для списка членов групп** — uid
- **Атрибут для аутентификации на терминальном сервере Linux** — uid
- **Атрибут для аутентификации на терминальном сервере Windows** — msDS-PrincipalName
- **Атрибут для поиска только измененных объектов** — modifyTimestamp
- Выключите опцию **Поддержка range для получения членов группы**.

8. Нажмите **[Далее]**.
9. На вкладке **Синхронизация**, укажите:
   - **Период синхронизации (мин.)**
   - Включите опцию **Инкрементальная синхронизация** для включения частичной синхронизации.

1. Опция **Инкрементальная синхронизация** и поле **Период инкрементальной синхронизации (мин.)** доступны только для LDAP-каталогов с типом **AD**.
2. Значение должно быть меньше периода полной синхронизации.

   - **Период инкрементальной синхронизации (мин.)**

10. Нажмите **[Далее]**.
11. На вкладке **Список серверов**:

Можно добавить адрес сервера LDAP

1. Нажмите ＋.
2. Укажите:
   - **Адрес** — IP-адрес или FQDN LDAP-сервера, например «termit-example-01.com».
   - **Протокол** — выберите из списка:

Перед выбором протоколов LDAP Over SSL и LDAP StartTLS добавьте доверенный сертификат,.

- **LDAP** — технология шифрования данных при подключении к LDAP-серверу не используется. Данные передаются в открытом виде по порту 389. Не рекомендуется использовать в продуктовых инсталляциях.
- **LDAP Over SSL** — защищенная версия протокола LDAP, которая использует технологию шифрования SSL/TLS при подключении к LDAP-серверу по порту 636.

        - **LDAP StartTLS** — защищенная версия протокола LDAP, при использовании которой сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование.
    - **Порт** — порт выбирается автоматически в зависимости от выбранного протокола. При необходимости параметр можно изменить.
3. Нажмите **[Сохранить]**.

Можно изменить адрес сервера LDAP

1. Наведите курсор на адрес сервера и нажмите ✎.
2. Измените:
    - **Адрес** — IP-адрес или FQDN LDAP-сервера, например «termit-example-01.com».
    - **Протокол** — выберите из списка:
        - **LDAP** — технология шифрования данных при подключении к LDAP-серверу не используется. Данные передаются в открытом виде по порту 389. Не рекомендуется использовать в продуктовых инсталляциях.
        - **LDAP Over SSL** — защищенная версия протокола LDAP, которая использует технологию шифрования SSL/TLS при подключении к LDAP-серверу по порту 636.
        - **LDAP StartTLS** — защищенная версия протокола LDAP, при использовании которой сначала устанавливается незащищенное соединение по порту 389, а затем отправляется запрос на шифрование.
    - **Порт** — порт выбирается автоматически в зависимости от выбранного протокола. При необходимости параметр можно изменить.
3. Нажмите **[Сохранить]**.

Можно удалить адрес сервера LDAP

1. Наведите курсор на адрес сервера и нажмите 🗑.
2. Чтобы подтвердить удаление, нажмите **[Да]**.

После подтверждения и сохранения новые настройки будут применены к LDAP-каталогу.

Удаление LDAP-каталога

Чтобы удалить LDAP-каталог:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги**.

3. Наведите курсор на полное имя каталога и нажмите ⋮.
4. Нажмите **[Удалить]**.
5. Нажмите **[Да]**.

LDAP-каталог будет удален.

После удаления LDAP-каталога пользователи не смогут:

- войти в портал администрирования;
- подключиться к десктоп-клиенту;
- запускать приложения в десктоп-клиенте.

Настройка Kerberos

Необходимые настройки описаны в статье Настройка Kerberos.

9.2.1. Настройка Kerberos

Kerberos необходим для реализации функции единого входа (SSO), чтобы пользователи могли войти в десктоп-клиент или на портал администрирования и запускать приложения без ввода учетных данных.

Kerberos можно настроить отдельно для каждого каталога. Если он не настроен, будет использоваться аутентификация по имени пользователя и паролю.

Настройка Kerberos состоит из нескольких этапов.

При использовании сквозной Kerberos-аутентификации в сценарии, когда пользователи и терминальные серверы размещены в разных доверенных доменах одного леса, требуется выполнить дополнительные настройки:

1. Добавьте все домены, в которых находятся пользователи и серверы, в раздел LDAP-каталоги Termit.
2. Для каждого добавленного домена загрузите keytab-файл, выпущенный на том домене, где размещены терминальные серверы.

1. Kerberos не работает на веб-клиентах.
2. Сценарий подключения десктоп-клиента на ОС Linux к ТС на ОС Windows с Kerberos недоступен, если ТС работают под

управлением Windows Server 2012, поскольку используемый при сквозной аутентификации Remote Credential Guard поддерживается начиная с Windows Server 2016.

Создание keytab-файла

AD

Чтобы сгенерировать keytab-файл, на контроллере домена:

1. Создайте сервисную учетную запись в домене, например krb-trm.
2. В свойствах учетной записи включите поддержу шифрования AES128 и AES256.
3. Сгенерируйте keytab-файл с помощью команды:

- После символа @ доменное имя должно быть указано заглавными буквами.
- Команда выполняется от имени администратора домена.

```
ktpass /out krb-trm.keytab /princ HTTP/internal.termit.local@TERMIT.LOCAL /pass *
/mapuser krb-trm@TERMIT.LOCAL /ptype KRB5_NT_PRINCIPAL /crypto AES256-SHA1
```

Где:

- krb-trm — имя сервисной учетной записи, созданной на шаге 1.
- krb-trm.keytab — целевой keytab-файл, сгенерированный на основе сервисной учетной записи krb-trm
- internal.termit.local — адрес портала внутреннего доступа
- TERMIT.LOCAL — доменное имя

Сгенерированный keytab-файл будет сохранен в текущей директории, в которой была выполнена команда, если не указан другой путь для вывода (например /out /path/to/directory/krb-trm.keytab). Далее полученный keytab-файл загрузите в настройках Kerberos.

Samba DC

Чтобы сгенерировать keytab-файл, на контроллере домена:

1. Создайте сервисную учетную запись в домене, например krb-trm:

```
sudo samba-tool user create krb-trm --description=Service account
```

Задайте пароль для сервисной учётной записи (будет запрошен интерактивно).

2. В свойствах учетной записи включите поддержу шифрования AES128 и AES256. Для этого:
   a. Отредактируйте атрибуты пользователя:

      ```
      sudo samba-tool user edit krb-trm
      ```

   b. В открывшемся текстовом редакторе добавьте или измените строку:

      ```
      msDS-SupportedEncryptionTypes: 24
      ```

      Сохраните изменения и выйдите из редактора.

      Значение 24 включает алгоритмы шифрования AES128 и AES256 и отключает устаревшие DES и RC4.

3. Добавьте SPN к сервисной учетной записи:

   ```
   sudo samba-tool spn add HTTP/internal.termit.local krb-trm
   ```

4. Сгенерируйте keytab-файл с помощью команды:

   ```
   sudo samba-tool domain exportkeytab krb-trm.keytab --principal=HTTP/internal.termit.local
   ```

   Где:

   - krb-trm.keytab — целевой keytab-файл, сгенерированный на основе сервисной учетной записи krb-trm;
   - internal.termit.local — адрес портала внутреннего доступа.

Сгенерированный keytab-файл будет сохранен в текущей директории, в которой была выполнена команда, если не указан другой путь для вывода (например /out /path/to/directory/krb-trm.keytab). Далее полученный keytab-файл загрузите в настройках Kerberos.

Чтобы сгенерировать keytab-файл, на сервере каталогов:

1. Создайте службу FreeIPA с именем брокера с помощью команды:

   ```
   ipa service-add --force --skip-host-check HTTP/internal.termit.local
   ```

   Где:

   - ipa — утилита командной строки для работы с FreeIPA;
   - service-add — команда для добавления нового сервиса в FreeIPA;
   - --force — принудительное добавление сервиса в FreeIPA;
   - --skip-host-check — пропуск проверки наличия хоста в IPA при добавлении сервиса;
   - HTTP/internal.termit.local — имя сервиса в формате тип/хост, где:
     - HTTP – тип сервиса (в данном случае - для веб-приложений);
     - internal.termit.local — адрес портала внутреннего доступа.

2. Сгенерируйте keytab-файл с помощью команды:

   ```
   ipa-getkeytab -p HTTP/internal.termit.local -k ~/krb_file.keytab
   ```

   Где:

   - ipa-getkeytab — утилита для получения (выгрузки) keytab-файла из FreeIPA;
   - -p HTTP/internal.termit.local — указывает principal (учетную запись Kerberos) в формате тип/хост, где:
     - HTTP – тип сервиса (для веб-приложений);
     - internal.termit.local – имя портала внутреннего доступа, для которого создается keytab-файл;
     - -k ~/krb_file.keytab — путь к файлу, в который будет сохранен keytab.

Далее полученный keytab-файл загрузите в настройках Kerberos.

Загрузка keytab-файла

Чтобы загрузить keytab-файл:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и наведите курсор на полное имя каталога.

3. Нажмите .
4. Чтобы включить использование Kerberos, активируйте опцию **Включить**.
5. Чтобы загрузить файл, нажмите на поле **keytab-файл**.
6. Нажмите **[Сохранить]**.

Keytab-файл будет загружен.

Настройка ТС

Настройка ТС ОС Linux

Для работы аутентификации по Kerberos на терминальных серверах под управлением Linux, включая поддерживаемые операционные системы (РЕД ОС, Astra Linux, Debian, ALT Linux, OpenSUSE):

1. В файле конфигурации `sshd (/etc/ssh/sshd_config)` в параметре `GSSAPIAuthentication`, укажите значение «yes».

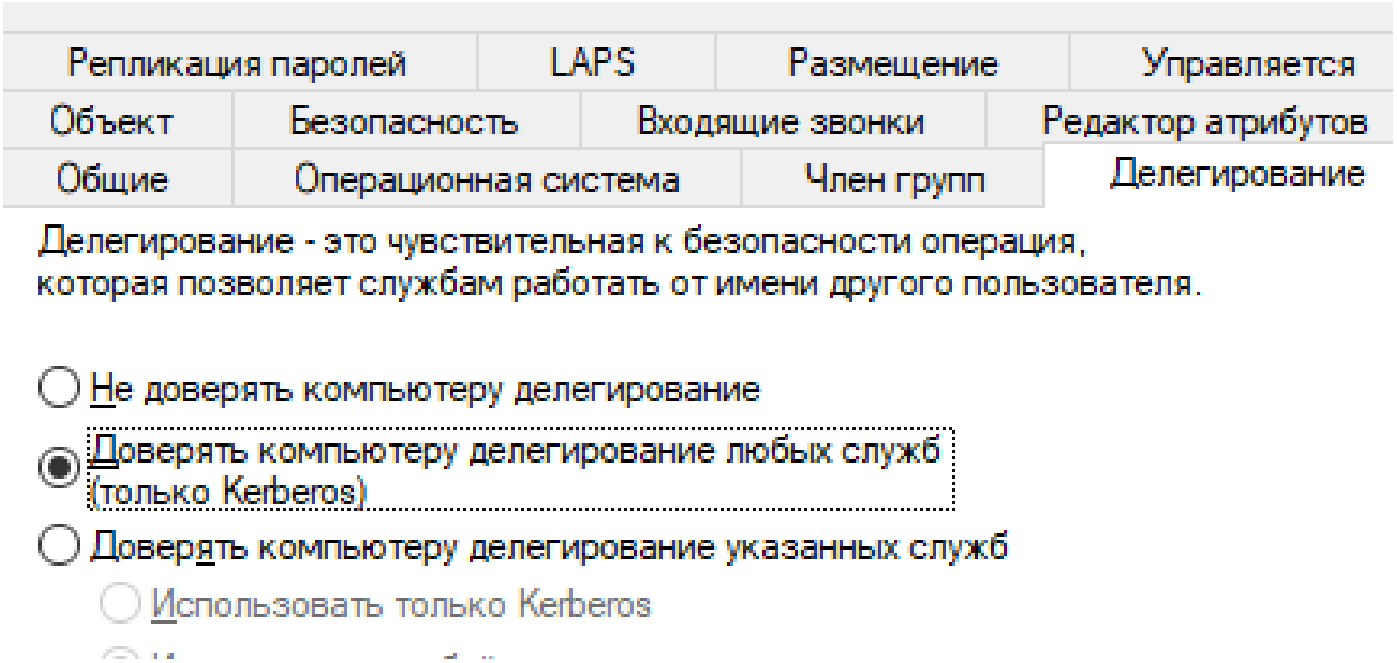
   В ALT Linux файл конфигурации sshd находится по пути: `/etc/openssh/sshd_config`.

2. В файле конфигурации `sshd (/etc/ssh/sshd_config)` параметр `AuthenticationMethods` должен быть задан в соответствии с рекомендациями.
3. Перезагрузите sshd с помощью команды:

   ```
   sudo systemctl restart sshd
   ```

4. В LDAP в свойствах объектов Linux терминальных серверов на вкладке **Делегирование** выберите **Доверять компьютеру делегирование любых служб (только Kerberos)**.

   Только для подключения с клиентских устройств под управлением ОС Windows.



Терминальный сервер будет настроен для работы аутентификации по Kerberos.

Настройка ТС ОС Windows

Для настройки аутентификации по Kerberos выполните следующие шаги:

1. Откройте редактор локальной групповой политики, выполнив команду в командной строке Windows (CMD):

```
gpedit.msc
```

2. Включите политики **Удаленный узел позволяет делегирование неэкспортируемых учетных данных** и **Ограничить делегирование учетных данных удаленным серверам** по следующему пути: **Конфигурации компьютера › Политики › Административные шаблоны › Система › Передача учетных данных**.
3. Убедитесь, что в десктоп-клиенте на ОС Linux в файле `/etc/krb5.conf` в секции `[libdefaults]` задан следующий параметр:

```
forwardable = true
```

На **Windows Server 2016** политика «Удаленный узел позволяет делегирование неэкспортируемых учетных данных» (Remote host allows delegation of non-exportable credentials) отсутствует. Для настройки делегирования выполните команду в командной строке Windows (CMD):

```
reg.exe add HKLM\SYSTEM\CurrentControlSet\Control\Lsa /v
```

```
DisableRestrictedAdmin /d 0 /t REG_DWORD /f
```

Настройка десктоп-клиента

Перед началом настройки убедитесь, что клиентское устройство, на которое установлен десктоп-клиент, и ТС введены в один домен.

Аутентификация на брокере Termit в браузере

Chrome

1. Создайте в каталоге **/etc/chromium/policies/managed/** файл **mydomain.json** с повышенными правами **root**, если он не был создан ранее, и добавьте в него параметры:

   ```
   {
   "AuthServerAllowlist": "*.termit.local",
   "AuthNegotiateDelegateAllowlist": "*.termit.local"
   }
   ```

2. Откройте в браузере Google Chrome страницу **chrome://policy** и проверьте, что настройки применились.

   [s chrome rules] | *s__chrome_rules.png*

   После успешной настройки авторизация в Termit будет выполнена без запроса ввода имени пользователя и пароля.

Firefox

1. Откройте браузер Mozilla Firefox и перейдите на страницу конфигурации **about:config**.
2. Добавьте параметр **.termit.local** для опций:
   - **network.negotiate-auth.trusted-uris**;
   - **network.automatic-ntlm-auth.trusted-uris**;
   - **network.negotiate-auth.delegation-uris**;

   [s firefox rules] | *s__firefox_rules.png*

3. Примените изменения и перезапустите браузер.

Аутентификация на Linux ТС Termit

Убедитесь, что на клиентском устройстве Linux в **/etc/krb5.conf** в **[libdefaults]** секции задан параметр **forwardable = true**.

Аутентификация на брокере Termit в десктоп-клиенте и браузере

1. Добавьте адрес портала внутреннего доступа в надежные сайты. В качестве примера будем рассматривать адрес **internal.termit.local**. Это можно сделать через групповые политики или настройки системы.
   - Групповые политики:
     a. Перейдите в **Конфигурация пользователя › Административные шаблоны › Компоненты Windows › Internet Explorer › Панель управления браузером › Вкладка «Безопасность» › Список назначений зоны для веб-сайтов**.
     b. Включите политику, нажмите **Показать...**.
     c. В поле **Имя значения** добавьте необходимый адрес, в нашем примере — **https://internal.termit.local/**.
     d. В поле **Значение** укажите **2** (это «Зона надёжных сайтов»).
   - Настройки системы:
     a. В **Панель управления › Сеть и Интернет › Свойства браузера › Безопасность** выберите **Надёжные сайты**, нажмите **Сайты** и добавьте необходимый узел в зону. В нашем примере — запись **https://internal.termit.local/**.
2. Включите опцию **Автоматический вход с текущим именем пользователя и паролем** в параметрах безопасности доверенных сайтов. Это можно сделать через групповые политики или настройки системы.
   - Групповые политики:
     a. Перейдите в **Конфигурация пользователя › Административные шаблоны › Компоненты Windows › Internet Explorer › Панель управления браузером › Вкладка «Безопасность» › Зона надежных сайтов › Параметры входа**.
     b. Включите политику и выберите в **Параметрах входа** опцию **Автоматический вход в сеть с текущим именем пользователя и паролем**.
   - Настройки системы:
     a. В **Панель управления › Сеть и Интернет › Свойства браузера › Безопасность** выберите **Надёжные сайты**, нажмите **Другой** и выберите опцию **Проверка подлинности › Ввод › Автоматический вход в сеть с текущим именем пользователя и паролем**.
3. Проверьте, что настройки применились и аутентификация без ввода учётных данных работает.

Аутентификация на брокере Termit в десктоп-клиенте и браузере будет работать без ввода учетных данных.

Аутентификация на Windows терминальном сервере Termit

1. Убедитесь, что аутентификация на брокере Termit в десктоп-клиенте осуществляется без ввода учётных данных.
2. В групповых политиках в разделе **Конфигурация компьютера › Административные шаблоны › Система › Передача учетных данных** настройте параметры **Разрешить передачу учетных данных, установленных по умолчанию** и **Разрешить передачу учетных данных, установленных по умолчанию, с проверкой подлинности сервера «только NTLM»**.

   Укажите в них SPN для терминальных серверов. Например:

   - `TERMSRV/terminal1.termit.local` — для включения Kerberos при доступе на сервер `terminal1.termit.local`.
   - `TERMSRV/*.termit.local` — для включения Kerberos при доступе ко всем серверам из домена `termit.local`.

9.3. Категории

Категория приложений — объединение приложений в одну группу для удобства работы с ними.

Администраторы могут управлять категориями приложений и списком всех категорий.

На вкладке **Категории** можно:

- Найти нужные категории приложений по имени, нажав .
- Обновить список категорий, нажав .
- Настроить видимость столбцов, нажав .

Создание новой категории

Чтобы создать категорию:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Категории** и нажмите **[Создать категорию]**

3. Задайте параметры категории:
   - **Имя категории** — отображаемое название категории в списке.
   - (Опционально) **Описание** — описание категории.
4. Нажмите **[Создать]**.

Категория будет создана.

Далее вы можете выбрать созданную категорию при добавлении приложения,.

Изменение настроек категории

Чтобы изменить настройки категории:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Категории**.
3. Наведите курсор на категорию и нажмите ✎.
4. Измените параметры категории:
   - **Имя категории** — отображаемое название категории в списке.
   - (Опционально) **Описание** — описание категории.
5. Нажмите **[Сохранить]**.

Параметры категории будут изменены.

Удаление категории

Чтобы удалить категорию:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Категории**.
3. Наведите курсор на категорию и нажмите ⋮.
4. Нажмите **[Удалить категорию]**.
5. Нажмите **[Да]**.

Категория будет удалена.

Для отмены действия нажмите **[Нет]**.

9.4. Внешний доступ

Чтобы пользователи могли подключаться к ТС вне внутренней сети, необходимо задать адрес портала внешнего доступа и настроить TLS шлюзы. После настроек внешних подключений:

- внешние пользователи будут проходить через отдельный балансировщик, расположенный в демилитаризованной зоне (DMZ);
- внешние пользователи будут использовать шлюз, расположенный в DMZ, для подключения к ТС;
- внутренние пользователи будут проходить через балансировщик во внутренней сети;
- прочие пользователи смогут подключаться к ТС напрямую, без шлюза.

Для передачи данных между десктоп-клиентом и шлюзом применяется протокол TLS версии не ниже 1.2.

Подробнее об архитектуре с внешними и внутренними пользователями.

На вкладке **Внешний доступ** можно:

- В блоке **Портал внешнего доступа** посмотреть информацию о настройках внешнего доступа, если он добавлен в Termit:
  - **Подключение** — информацию об адресе портала внешнего доступа и общедоступном адресе.
  - **Сертификат** — информацию о сертификате: общее имя, альтернативные имена, отпечаток сертификата, срок действия и издателя.
- В блоке **Шлюзы удаленного доступа**:
  - Обновить список шлюзов, нажав ↻.

В версии 2.5 Termit прекращена поддержка SSH-шлюза. Все добавленные ранее SSH-шлюзы отображаются в списке шлюзов. Их можно только удалить.

  - Настроить видимость столбцов, нажав ⊞.
  - Добавить новый шлюз.
  - Удалить шлюз.

Настройка внешнего подключения

Чтобы настроить внешнее подключение:

После включения настроек, изменения адреса или сертификатов сервисы брокера будут перезагружены, и он будет недоступен в течение не более 5 минут.

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Внешний доступ** и нажмите **[Настроить внешний доступ]**.
3. Включите опцию **Портал внешнего доступа**. После этого будут доступны к заполнению следующие поля:
   - В параметре **Общедоступный адрес** укажите FQDN-адрес портала внешнего доступа. Он должен отличаться от FQDN-адреса портала внутреннего доступа который был указан при развертывании брокера или при изменении настроек HTTPS.
   - Загрузите сертификат, выданный для указанного FQDN. Сертификат потребуется только в том случае, если вы включаете эти настройки или меняете адрес портала внешнего доступа.
   - Загрузите закрытый ключ, выданный для указанного FQDN, в формате `.key`.
   - Укажите IP-адрес балансировщика, которому будет разрешен доступ.

     Ниже отобразится блок **Информация о сертификате** с полной информацией об устанавливаемом сертификате.
4. Нажмите **[Сохранить]**.

Настройка внешнего подключения будет завершена.

Далее добавьте шлюз и настройте балансировщик нагрузки.

1. Балансировщик нагрузки для внешних подключений следует настроить таким образом, чтобы он перенаправлял запросы с порта 443 на порт 10443, где установлен брокер.
2. При открытии сессии через шлюз и при отсутствии TLS-шлюза система выдает ошибку **Нет доступных включенных шлюзов**.

Добавление шлюза

Для добавления нового шлюза удаленного доступа:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Внешний доступ** и нажмите **[Добавить шлюз]**.
3. На вкладке **Добавление шлюза**:
   - **Внешний адрес** — укажите FQDN-имя шлюза — при обращении внешних пользователей (через интернет).
   - **Внешний порт шлюза** — укажите внешний порт шлюза.
   - **Внутренний адрес** — укажите FQDN-имя шлюза — при обращении брокер-серверов из внутренней сети.
   - (Опционально) **Описание** — добавьте описание шлюза.
4. Нажмите **[Добавить]**.
5. На вкладке **Установка агента** скопируйте указанную команду в надежное место. Она понадобится после установки дополнительного ПО на ТС.

   Вы можете скопировать команду установки агента позже. Подробнее в разделе Установка агента.

6. Нажмите **[Закрыть]**.

Шлюз удаленного доступа появится в списке.

Перевод шлюза в режим обслуживания

Когда шлюз находится на обслуживании, можно проводить на нем плановые работы. Чтобы перевести шлюз в режим обслуживания:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Внешний доступ**.
3. Наведите курсор на нужный шлюз и нажмите .
4. Нажмите **[Да]**.

Статус шлюза изменится на «На обслуживании». При включении статуса «На обслуживании» шлюз со стороны системы Termit будет недоступен.

Перевод шлюза из режима обслуживания

Чтобы перевести шлюз из режима обслуживания:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Внешний доступ**.
3. Наведите курсор на нужный шлюз в статусе «На обслуживании» и нажмите 🔧.
4. Нажмите **[Да]**.

Статус шлюза изменится на «Активен», шлюз со стороны системы Termit будет доступен.

Удаление шлюза

Чтобы удалить шлюз:

1. На портале администрирования в левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Внешний доступ**.
3. Наведите курсор на шлюз и нажмите ⋮.
4. Нажмите **[Удалить шлюз]**.
5. Нажмите **[Да]**.

Шлюз будет удален. После удаления шлюза внешние пользователи не смогут запустить сессию, но при этом могут подключиться к брокеру и запустить десктоп клиент.

9.5. Зоны

Здесь находится описание, как добавлять, изменять и удалять зоны доступа пользователей к приложениям.

Зона – это набор подсетей, который может использоваться для разграничения доступа пользователей к приложениям в зависимости от IP адреса их клиентского устройства.

На вкладке **Зоны** можно добавлять, изменять и удалять зоны. Удалять зону можно, только если она не используется в фильтрах доступа к приложению.

Добавление зоны

Чтобы добавить зону:

1. На портале администрирования в разделе **Настройки** перейдите на вкладку **Зоны**.
2. Нажмите **[+ Добавить зону]**.
3. Задайте параметры для добавления зоны:
   - **Имя** - укажите имя зоны доступа к приложениям.
   - **Списки подсетей** - укажите одну или несколько подсетей в формате `адрес подсети/маска подсети`. Например, `192.168.1.0/24`
4. Нажмите **[Добавить]**.

Зоны доступа будут доступны для выбора при создании фильтров доступа к приложению с атрибутом Зона при добавлении и изменении приложения.

Редактирование зоны

Чтобы изменить зону:

1. На портале администрирования в разделе **Настройки** перейдите на вкладку **Зоны**.
2. Выберите нужную зону и нажмите .
3. Измените параметры зоны.
4. Нажмите **[Сохранить]**.

Новые настройки будут применены к зоне.

Удаление зоны

Чтобы удалить зону:

1. На портале администрирования в разделе **Настройки** перейдите на вкладку **Зоны**.
2. Выберите нужную зону и нажмите .
3. Нажмите **[Удалить]**.

Зона будет удалена.

Глава 10. Брокеры

В разделе **Брокеры** можно:

- Посмотреть информацию о брокере:
  - имя, которое было задано при установке;
  - статусы «Работает» и «Не работает». В случае недоступности брокера более 5 минут его статус изменяется на «Не работает»;
  - версия брокера;
  - время последней доступности «Последний пульс».
- Обновить список брокеров, нажав ↻.
- Настроить видимость столбцов, нажав ⫼.
- Экспортировать данные в CSV, нажав ⋮.

Удаление брокера

Перед удалением брокера в портале администрирования необходимо сначала его деинсталлировать,.

1. На портале администрирования в левом меню выберите раздел **Брокеры**.
2. Наведите курсор на брокер и нажмите ⋮.
3. Нажмите **[Удалить брокер]**.
4. Нажмите **[Да]**

Брокер будет удален.

Для отмены действия нажмите **[Нет]**.

Экспорт данных в CSV

Чтобы выполнить экспорт данных в CSV:

1. На портале администрирования в левом меню выберите раздел **Брокеры**.
2. Нажмите ⋮.
3. Нажмите **[Экспорт CSV]**.

4. Выберите данные для экспорта.
5. Нажмите **[Экспорт]**.

Выбранные данные будут экспортированы в файл CSV-формата.

Глава 11. Пользователи

В разделе **Пользователи** отображается список пользователей, которые хоть раз выполнили вход в систему (портал администратора, веб- или десктоп-клиент).

Пользователи — внутренние и внешние пользователи, которые могут запускать приложения, и администраторы, которые могут настраивать Termit.

На странице можно:

- Найти нужного пользователя по имени учетной записи, каталогу, статусу и активным сессиям, нажав .
- Обновить список пользователей, нажав .
- Настроить видимость столбцов, нажав .
- Экспортировать данные в CSV, нажав .

Пользователи

- «tadm» — создается системой по умолчанию, имеет административные права для управления и первоначальной настройки компонентов и не привязан к LDAP. Например, такой пользователь может помочь починить LDAP, указав другой LDAP-сервер или изменив иные параметры, когда LDAP недоступен.
- «system» — создается системой по умолчанию. От имени этого пользователя в журнале событий отображается запись операций в фоновом режиме.

Просмотр информации о пользователе

Чтобы просмотреть информацию о пользователе:

1. На портале администрирования в левом меню выберите раздел **Пользователи**.
2. Наведите курсор на нужного пользователя и нажмите на имя пользователя.

На странице отобразятся доступные приложения, сессии, события и роли, назначенные на пользователя.

Блокировка пользователя

Блокировка пользователя применяется, когда нужно быстро ограничить его доступ к системе. При этом он блокируется локально, а не в LDAP.

Чтобы заблокировать пользователя:

1. На портале администрирования в левом меню выберите раздел **Пользователи**.
2. Наведите курсор на пользователя со статусом «Активен» и нажмите ⊘. Также можно нажать на имя пользователя и в правом верхнем углу нажать **[Заблокировать]**.
3. Нажмите **[Заблокировать]**.

   Для отмены действия нажмите **[Отменить]**.

Пользователь будет заблокирован, статус изменится на «Заблокирован», доступ к системе будет ограничен.

Разблокировка пользователя

Чтобы разблокировать пользователя:

1. На портале администрирования в левом меню выберите раздел **Пользователи**.
2. Наведите курсор на пользователя со статусом «Заблокирован» и нажмите ⊘.
3. Нажмите **[Разблокировать]**.

   Для отмены действия нажмите **[Отменить]**.

Пользователь будет разблокирован, статус изменится на «Активен», появится доступ к системе.

Закрытие сессий пользователя

Чтобы закрыть все сессии пользователя:

1. На портале администрирования в левом меню выберите раздел **Пользователи**.
2. Наведите курсор на пользователя и нажмите ×. Также можно нажать на имя пользователя и в правом верхнем углу нажать **[Закрыть сессии пользователя]**.
3. Нажмите **[Закрыть]**.

   Для отмены действия нажмите **[Отменить]**.

Все сессии у пользователя будут закрыты.

Экспорт данных в CSV

Чтобы выполнить экспорт данных в CSV:

1. На портале администрирования в левом меню выберите раздел **Пользователи**.
2. Нажмите кнопку ⋮.
3. Нажмите **[Экспорт CSV]**.
4. Выберите данные для экспорта.
5. Нажмите **[Экспорт]**.

Выбранные данные будут экспортированы в файл формата `.csv` на ПК.

Глава 12. Права доступа

В разделе **Права доступа** администратор задаёт, какие действия пользователи могут выполнять в Termit и над какими объектами.

Доступ собирается из роли, области видимости и назначения. Роль определяет разрешённые операции над типами объектов. Область видимости ограничивает эти операции всеми объектами выбранного типа или отдельными экземплярами. Назначение связывает роль и область видимости с пользователями или группами LDAP, а итоговые права пользователя складываются из всех его назначений.

Подробнее о настройках:

- Роли.
- Области видимости.
- Назначения.
- Выражения SpEL в областях видимости.

12.1. Назначения

В этом разделе описано как управлять назначениями для выдачи доступа пользователям.

Назначение — это правило доступа, которое включает три обязательных атрибута: роль (определяет допустимые операции), область видимости (устанавливает границы применения роли) и перечень LDAP-пользователей или групп (определяет субъектов, получающих доступ).

Доступ выдаётся в три шага: подготовка роли и области, затем создание назначения с привязкой к пользователям или группам. Конечные права пользователя складываются из всех активных назначений, в которых он фигурирует.

Создание назначения

Чтобы создать назначение:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Назначения**.
2. Нажмите на **[+ Создать назначение]**.
3. Задайте параметры для создания назначения:

- **Имя** - имя назначения
- (Опционально) **Описание** - описание назначения.
- **Роль** - выберите необходимую роль или создайте новую в разделе Роли,.
- **Область видимости** - выберите необходимую область видимости или создайте новую в разделе Области видимости,.
- В блоке **Назначить для** выберите пользователей и группы LDAP, получающие доступ.

4. Нажмите **[Добавить]**.

Клонирование назначения

Клонирование назначения предназначено для быстрого создания нового назначения на основе существующего с автоматическим копированием всех параметров и предзаполненными полями, что позволяет сэкономить время при внесении точечных изменений в настройки доступа.

Чтобы клонировать назначение:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Назначения**.
2. Выберите нужное назначение и нажмите .
3. Задайте параметры для клонируемого назначения:
   - **Имя** - по умолчанию указывается имя клонируемого назначения с добавлением в начале «Копия», например «Копия Назначение». Измените название назначения.
   - (Опционально) **Описание** - измените описание клонируемого назначения.
   - **Роль** - выберите необходимую роль.
   - **Область видимости** - выберите необходимую область видимости.
   - В блоке **Назначить для** выберите пользователей и группы LDAP, получающие доступ.
4. Нажмите **[Добавить]**.

Клон назначения будет создан.

Изменение назначения

Изменение назначения предназначено для быстрого изменения параметров назначения.

Чтобы изменить назначение:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Назначения**.
2. Выберите нужное назначение и нажмите .
3. Измените параметры назначения:
   - **Имя** - измените название назначения.
   - (Опционально) **Описание** - измените описание назначения.
   - **Роль** - добавьте или удалите необходимую роль.
   - **Область видимости** - добавьте или удалите область видимости.
   - В блоке **Назначить для** добавьте или удалите пользователей и группы LDAP, получающие доступ.
4. Нажмите **[Сохранить]**.

Назначение будет изменено.

Удаление назначения

Чтобы удалить назначение:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Назначения**.
2. Выберите нужное назначение и нажмите ⋮.
3. Нажмите **[Удалить назначение]**.
4. Нажмите **[Да]**.

Назначение будет удалено.

12.2. Роли

Здесь можно посмотреть описание действий на вкладке "Роли".

Роль — это именованный набор прав, который определяет, какие операции (CRUD + Execute) и над какими типами объектов/ресурсов разрешены пользователю.

В разделе **Роли** можно:

- Найти нужную роль по имени, нажав .
- Обновить список ролей, нажав .

- Настроить видимость столбцов, нажав ⫼.
- Посмотреть подробную информацию о роли.
- Клонировать роль.

Создание роли

Чтобы создать роль:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Роли**.
2. В правом верхнем углу нажмите на **[Создать роль]**.
3. На вкладке **Общие настройки** задайте параметры для создания роли:
   - **Имя** - имя роли.
   - (Опционально) **Описание** - описание роли.
4. Нажмите **[Далее]**.
5. На вкладке **Права** выберите права доступа, установив флажки напротив нужных действий (CRUD + Execute) для разделов **Мониторинг**, **Ресурсы**, **Администрирование**, **Управление доступом**.
6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию о роли и нажмите **[Создать]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Роль будет создана.

Клонирование роли

Клонирование роли предназначено для быстрого создания новой роли на основе существующей с автоматическим копированием всех прав и предзаполненными полями, что позволяет сэкономить время при внесении точечных изменений в настройки доступа.

Чтобы клонировать роль:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Роли**.
2. Выберите нужную роль и нажмите ⧉.
3. На вкладке **Общие настройки** задайте параметры для клонируемой роли:
   - **Имя** - по умолчанию указывается имя клонируемой роли с добавлением в начале «Копия», например «Копия Администратор». Измените название роли.

- (Опционально) **Описание** - измените описание клонируемой роли.

4. Нажмите **[Далее]**.
5. На вкладке **Права** добавьте права доступа, установив или убрав флажки напротив действий (CRUD + Execute) для разделов **Мониторинг**, **Ресурсы**, **Администрирование**, **Управление доступом**.
6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию о клонируемой роли и нажмите **[Добавить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Клон роли будет создан.

Изменение роли

Изменение роли предназначено для быстрого изменения настроек доступа к ресурсам для роли.

Чтобы изменить роль:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Роли**.
2. Выберите нужную роль и нажмите ✎.
3. На вкладке **Общие настройки** измените параметры роли
   - **Имя** - измените название роли.
   - (Опционально) **Описание** - измените описание роли.
4. Нажмите **[Далее]**.
5. На вкладке **Права** добавьте права доступа, установив или убрав флажки напротив действий (CRUD + Execute) для разделов **Мониторинг**, **Ресурсы**, **Администрирование**, **Управление доступом**.
6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию о роли и нажмите **[Сохранить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Роль будет изменена.

Удаление роли

Чтобы удалить роль:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Роли**.
2. Выберите нужную роль и нажмите ⋮.
3. Нажмите **[Удалить роль]**.
4. Нажмите **[Да]**.

Роль будет удалена.

12.3. Области видимости

Здесь можно посмотреть описание действий на вкладке "Области видимости".

Область видимости определяет границы применения прав роли: можно либо разрешить доступ ко всем объектам выбранного типа, либо ограничить его конкретными экземплярами через ручной выбор из списка.

В разделе **Области видимости** можно:

- Найти нужную область видимости по имени, нажав ⏷.
- Обновить список областей видимости, нажав ↻.
- Настроить видимость столбцов, нажав ▥.
- Посмотреть подробную информацию об области видимости.
- Клонировать область видимости.

Создание области видимости

Чтобы создать область видимости:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Область видимости**.
2. В правом верхнем углу нажмите на **[Создать область видимости]**.
3. На вкладке **Общие настройки** задайте параметры для создания области видимости:
   - **Имя** - имя области видимости.
   - (Опционально) **Описание** - описание области видимости.
4. Нажмите **[Далее]**.
5. На вкладке **Область видимости** выберите объекты, для которых будут разрешены действия, установив флажки напротив нужных объектов.

При выборе значения **Все объекты** будут разрешены действия для всех объектов.

6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию об области видимости и нажмите **[Создать]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Область видимости будет создана.

Клонирование области видимости

Клонирование области видимости предназначено для быстрого создания области на основе существующей с автоматическим копированием всех значений и предзаполненными полями, что позволяет сэкономить время при внесении точечных изменений в настройку.

Чтобы клонировать область видимости:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Область видимости**.
2. Выберите нужную область видимости и нажмите .
3. На вкладке **Общие настройки** задайте параметры для клонируемой области видимости:
   - **Имя** - по умолчанию указывается имя клонируемой области с добавлением в начале «Копия», например «Копия Область видимости». Измените название области видимости.
   - (Опционально) **Описание** - измените описание клонируемой области видимости.
4. Нажмите **[Далее]**.
5. На вкладке **Область видимости** добавьте объекты, для которых будут разрешены действия, установив или убрав флажки напротив нужных полей.

   При выборе значения **Все объекты** будут разрешены действия для всех объектов.

6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию о клонируемой области видимости и нажмите **[Добавить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Клон области видимости будет создан.

Изменение области видимости

Изменение области видимости предназначено для быстрого изменения настроек доступа к ресурсам для роли.

Чтобы изменить область видимости:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Области видимости**.
2. Выберите нужную область видимости и нажмите ✎.
3. На вкладке **Общие настройки** измените параметры области видимости
   - **Имя** - измените название области видимости.
   - (Опционально) **Описание** - измените описание области видимости.
4. Нажмите **[Далее]**.
5. На вкладке **Область видимости** добавьте объекты, для которых будут разрешены действия, установив или убрав флажки напротив нужных полей.

   При выборе значения **Все объекты** будут разрешены действия для всех объектов.

6. Нажмите **[Далее]**.
7. На вкладке **Подтверждение** проверьте информацию об области видимости и нажмите **[Сохранить]**. При необходимости вы можете вернуться на предыдущие шаги и изменить параметры.

Область видимости будет изменена.

Удаление область видимости

Чтобы удалить область видимости:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Область видимости**.
2. Выберите нужную область видимости и нажмите ⋮.
3. Нажмите **[Удалить область видимости]**.
4. Нажмите **[Да]**.

Область видимости будет удалена.

12.4. Выражения SpEL в областях видимости

Помимо выбора объектов из списка, доступ в области видимости можно задать выражением на языке Spring Expression Language (SpEL). Выражение вычисляется для каждого объекта. В область видимости попадают и объекты, созданные после настройки. Добавлять такие объекты вручную не требуется.

Задание выражения

Чтобы задать выражение:

1. На портале администрирования в разделе **Права доступа** перейдите на вкладку **Области видимости**.
2. Создайте область видимости или выберите существующую для изменения.
3. На шаге **Область видимости** в списке найдите нужную строку и нажмите **[Перейти к расширенной настройке]**.
4. Введите выражение в открывшемся окне и сохраните изменения.
5. Завершите создание или изменение области видимости.

Принцип работы

- Для проверяемого объекта выбирается выражение, заданное для его типа.
- Выражение вычисляется по правилам SpEL.
- Если результат равен `true`, объект входит в область видимости.

Таблица 6. Переменные

Переменная	Описание
`asset`	Проверяемый объект со своими свойствами. Набор свойств зависит от типа объекта
`operation`	Проверяемая операция, например создание или удаление
`#scope`	Массив объектов, выбранных флажками в этой области видимости. Содержит объекты всех типов, доступ к которым разрешен в области

Таблица 7. Функции

Функция	Возвращает `true`, если
`contains(array, value)`	массив `array` содержит значение `value`
`containsAll(array1, array2)`	все элементы `array2` входят в `array1`

Функция	Возвращает `true`, если
`containsAny(array1, array2)`	хотя бы один элемент `array2` входит в `array1`
`containsNone(array1, array2)`	ни один элемент `array2` не входит в `array1`

Массив можно получить из `#scope` или объявить в выражении, например {'RDS'}.

Выражение с массивом из `#scope`:

```
contains(#scope, asset)
```

Выражение с массивом, заданным в выражении:

```
contains({'RDS'}, asset.serverType)
```

Свойства объектов

У всех объектов есть свойства `id` (UUID) и `assetType` (тип объекта). Дополнительные свойства приведены в таблице.

Таблица 8. Дополнительные свойства

Тип (`assetType`)	Свойства
`RoleDefinition` — Роль	`name`
`AccessScope` — Область видимости	`name`
`AccessBinding` — Назначение	`name`
`DeliveryGroup` — Группа доставки	`name` `operationSystemType` (`LINUX`) `serverType` (`RDS`)
`MachineCatalog` — Каталог ресурсов	`name` `operationSystemType` (`LINUX`) `serverType` (`RDS`)

Тип (`assetType`)	Свойства
`Resource` — Приложение	`name` `appPath` — путь к приложению `status` (`ON`, `OFF`) `type` (`APP`, `DESKTOP`) `os` (`LINUX`)
`ResourceCategory` — Категория приложений	`name`
`TrustedCertificate` — Доверенный сертификат	Дополнительных свойств нет
`SystemSettings` — Системные настройки	`key` — ключ настройки
`User` — Пользователь	`username` — логин `superuser`, `locked`, `isLocal` (`true`, `false`) — признаки суперпользователя, блокировки и локальной учетной записи `ldapGroupIds` — идентификаторы LDAP-групп пользователя `ldapCatalog` — LDAP-каталог пользователя

`Broker` — Брокер	`brokerId`
	
	`name`

`TermitGateway` — Шлюз удаленного доступа	`address` `status` (`ACTIVE`, `MAINTENANCE`)
`LdapCatalog` — LDAP-каталог	`name`
`Policy` — Политика	`name` `status` (`OFF`, `DRAFT`, `MODELING`, `ON`) `global` — глобальная политика `default` — политика по умолчанию `targets` — цели политики (`id`, `type`, `name`) `types` — типы настроек политики
`Zone` — Зона	`name`

Допустимые значения `SystemSettings.key`:

```
AuthSettings
CasInternalSettings
EventDepth
ExternalGatewaySettings
ExternalHttpsSettings
FullRoleSettings
GatewaySettings
HttpsSettings
InstallationFileSettings
KerberosSettings
LDAPSettings
LdapCatalogsSettings
LocalUserLockSettings
MfaBypass
MfaSettings
PasswordSettings
PrometheusInternalSettings
RadiusSettings
RoleSettings
RsyslogSettings
SessionDepth
SmartCardSettings
TerminalServerRootCertificateSettings
TerminalServerSettings
TokenSettings
UserAppearance
WebClientSettings
```

Допустимые значения `Policy.types`:

```
CLIPBOARD_REDIRECTING
SOUND_REDIRECTION
FILE_SYSTEM_REDIRECTION
SMART_CARD_REDIRECTION
HOME_DIRECTORY_PATH
ROAMING_PROFILES
LOCAL_PRINTERS
SESSION_MANAGEMENT_ACCESS
REMOTE_APP_WITH_FREE_RDP
CLIENT_TIME_ZONE_REDIRECTION
CONCURRENT_SESSIONS_LIMIT
CONCURRENT_OPENING_SESSIONS_LIMIT
CPU_USAGE_LIMIT
DISK_USAGE_LIMIT
MEMORY_USAGE_LIMIT
BASIC_MEMORY_USAGE_LIMIT
```

Примеры

Группы доставки с типом сервера RDS

Требуется предоставить доступ ко всем существующим и будущим группам доставки с типом сервера `RDS`.

```
asset.serverType == 'RDS'
```

Допустимо перечислить значения в массиве:

```
contains({'RDS'}, asset.serverType)
```

Объекты, имя которых соответствует шаблону

Требуется предоставить доступ ко всем группам доставки, имена которых начинаются с `finance`. Для этого задайте регулярное выражение:

```
asset.name matches '^finance.*'
```

Каталоги ресурсов с ОС Windows

Требуется предоставить доступ ко всем каталогам ресурсов с операционной системой Windows.

```
asset.operationSystemType == 'WINDOWS'
```

Рекомендации

- Строковые значения записываются в одинарных кавычках, например 'RDS' и 'WINDOWS'.
- В выражении доступны только свойства проверяемого типа объекта. Например, `serverType` есть у групп доставки и каталогов ресурсов и отсутствует у приложений.
- Для выражений с `#scope` нужный объект должен быть выбран флажком в этой же области видимости.

Глава 13. Профили пользователей

13.1. Настройка профиля пользователя в терминальной среде Windows

Перемещаемые профили позволяют пользователям получить доступ к своему профилю независимо от того, к какому именно ТС он подключился. Профиль пользователя включает настройки программ, документы, ветви реестра и прочие настройки, файлы и параметры. При выходе из системы все измененные настройки профиля и документы синхронизируются с файловым сервером.

В этом разделе описано, как настроить перемещаемые профили (roaming profiles) на компьютерах пользователей в домене Active Directory (AD) с помощью групповых политик (GPO) для группы доступа пользователей домена.

1. Для ускорения загрузки профиля пользователя помимо перемещаемых профилей рекомендуется также настроить перенаправление папок. Подробнее о настройке перенаправления папок можно прочесть на официальном сайте Microsoft.
2. Рекомендуется самостоятельно или при помощи сторонних специалистов спланировать архитектуру перемещаемых профилей, подходящую вашей организации. Ниже описан пример одного из вариантов настройки.

1. При использовании перемещаемых профилей на ТС под управлением Windows Server 2012 R2 сделайте следующее:
   a. В разделе **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ProfSvc\Parameters** добавьте новый ключ **UseProfilePathExtensionVersion** со значением 1 с помощью команды:

   ```
   reg add "HKLM\SYSTEM\CurrentControlSet\Services\ProfSvc\Parameters" /v
   UseProfilePathExtensionVersion /d 1 /t REG_DWORD
   ```

   b. Перезагрузите ТС.
2. Создайте в домене AD группу безопасности «RoamingProfilesGroup» и добавьте в нее пользователей и ТС, для и на которых будут использоваться Перемещаемые профили, с

помощью консоли Active Directory Users and Computers (ADUC).

3. С помощью проводника Windows создайте и опубликуйте на файловом сервере сетевую папку, в которой будут храниться перемещаемые профили:
   a. На файловом сервере создайте новую папку и назовите ее, например «RoamingProfiles».
   b. Предоставьте полный доступ (чтение/запись) для **Authenticated users** .
   c. В свойствах папки перейдите на вкладку **Безопасность (Security)**, нажмите **[Дополнительно]** (**[Advanced]**), затем нажмите **[Отключение наследования]** (**[Disable Inheritance]**).
   d. В открывшемся окне выберите **Преобразовать унаследованные разрешения в явные разрешения этого объекта (Convert inherited permissions into explicit permissions on the object)**.
   e. В списке разрешений NTFS оставьте права:
      - СИСТЕМА (Полный доступ, Для этой папки, ее подпапок и файлов) (SYSTEM (Full control, This folder, subfolders and files))
      - Администраторы (Полный доступ, Для этой папки, ее подпапок и файлов) (Administrators (Full control, This folder, subfolders and files))
      - СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ (Полный доступ, Только для подпапок и файлов) (CREATOR OWNER (Full control, Subfolders and files only))
      - RoamingProfilesGroup (Содержание папки/ чтение данных, Создание папок/ дозапись данных, Только для этой папки) (RoamingProfilesGroup (Folder contents/reading data, Creating folders/writing additional data, This folder))
4. Создайте в домене AD групповую политику, например «RoamingProfilesGPO».
5. Для групповой политики «RoamingProfilesGPO»:
   a. Из фильтров безопасности «RoamingProfilesGPO» удалите **Authenticated users** и добавьте группу безопасности «RoamingProfilesGroup».
   b. Перейдите на вкладку **Делегирование** (**Delegation**) и добавьте **Authenticated users** с разрешением на чтение (**Read**).
6. Откройте групповую политику «RoamingProfilesGPO» для редактирования, перейдите в **Конфигурация компьютера › Политики › Административные шаблоны › Система › Профили пользователей** (**Computer Configuration › Policies › Administrative Templates › System › User Profiles**), включите параметр **Установить путь к перемещаемым профилям для всех пользователей, входящих в систему на данном компьютере** (**Set roaming profile path for all users logging onto this computer**) и укажите в качестве его значения

UNC-путь до сетевой папки с профилями пользователей, например **\\fileserver.termit.local\RoamingProfiles\%username%**.

Путь до папки **\\fileserver.termit.local\RoamingProfiles** используется в качестве примера. Необходимо заменить его на актуальный.

7. Привяжите групповую политику «RoamingProfilesGPO» к Organizational Unit, где располагаются ТС.
8. Включите связь (**Link enabled**).

Настройка перемещаемых профилей (roaming profiles) на компьютерах пользователей в домене Active Directory (AD) будет завершена.