Категории

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

Администраторы могут управлять категориями приложений и списком всех категорий.

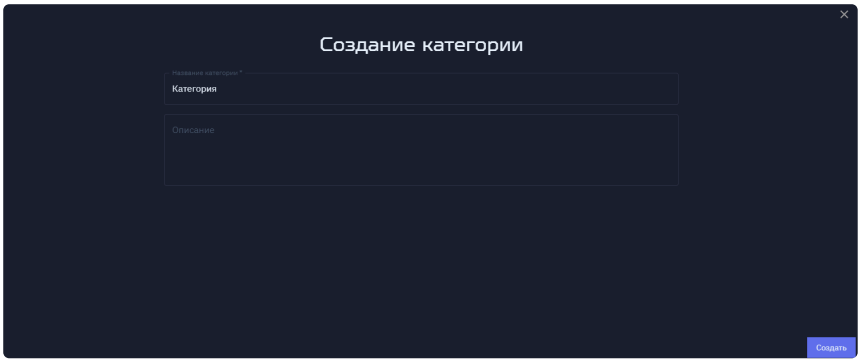
На вкладке **Категории** можно:

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

Создание новой категории

Чтобы создать категорию:

1. В левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **Категории** и нажмите **[Создать категорию]**
3. Задайте параметры категории:
   - **Название категории** — отображаемое название категории в списке.
   - (Опционально) **Описание** — описание категории.



4. Нажмите **[Создать]**.

Категория создана.

Далее вы можете выбрать созданную категорию при добавлении приложения.

Изменение настроек категории

Чтобы изменить настройки категории:

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

Параметры категории изменены.

Удаление категории

Чтобы удалить категорию:

1. 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 удалена.

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

Общие настройки

В этом разделе содержатся различные инструкции по настройке системы СТД «Термит».

HTTPS

Чтобы изменить адрес брокера, загрузить ключ, сертификат и цепочку сертификатов:

1. В разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **HTTPS** и нажмите ✎.
2. При необходимости измените адрес брокера.
3. Чтобы загрузить сертификат или цепочку сертификатов, нажмите на поле **Сертификат**.
4. Чтобы загрузить закрытый ключ, нажмите на поле **Закрытый ключ**.
5. Нажмите **[Сохранить]**.

Настройки сохранены.

Подробнее о генерации самоподписанного сертфиката.

Внешний вид десктоп-клиента

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

1. 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 разделены по типу в десктоп-клиенте.

Внешние подключения

Настройка

Чтобы пользователи могли подключаться к терминальным серверам вне внутренней сети, необходимо задать отдельный (внешний) адрес брокера и настроить SSH-шлюз. 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 терминальным серверам;
- прочие пользователи будут проходить через балансировщик во внутренней сети;
- прочие пользователи смогут подключаться к терминальным серверам напрямую, без шлюза.

Подробнее об архитектуре с внешними и внутренними пользователями.

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. В разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Внешние подключения** и нажмите ✎.
2. На вкладке **Базовые параметры для HTTPS**:
   a. Чтобы настроить внешнее подключение, активируйте опцию **Включить**.
   b. В параметре **Общедоступный адрес** укажите FQDN брокера. Он должен отличаться от FQDN брокера, который был указан при развертывании брокера или при изменении настроек HTTPS.
   c. Загрузите сертификат, выданный для указанного FQDN. Сертификат потребуется только в том случае, если вы включаете эти настройки или меняете внешний адрес брокера. Если меняются только настройки шлюзов, то сертификат не нужен.
   d. Загрузите закрытый ключ, выданный для указанного FQDN.
   e. В параметре **Время жизни сертификата (сек.)** задайте срок действия временного сертификата.
   f. Нажмите **[Далее]**.
3. На вкладке **Шлюзы удаленного доступа** нажмите ＋.
4. Задайте параметры:
   - **Адрес** — IP-адрес;
   - **Порт** — по умолчанию TCP-порт 22.
5. Нажмите **[Сохранить]**.

Шлюз удаленного доступа появится в списке.

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

Далее настройте балансировщик нагрузки.

Балансировщик нагрузки для внешних подключений следует настроить таким образом, чтобы он перенаправлял запросы с порта 443 на порт 10443, где установлен брокер.

Скачивание корневого сертификата

При запуске терминальной сессии брокер создает временный сертификат и закрытый ключ. Когда десктоп-клиент подключается к шлюзу удаленного доступа, он использует сертификат и закрытый ключ, предоставленные брокером. Срок действия временного сертификата можно задать в настройках внешнего подключения.

Аутентификация на SSH-шлюзе выполняется по сертификату, что повышает безопасность системы и снижает вероятность атак злоумышленников.

Чтобы скачать корневой сертификат и установить его на шлюзе:

1. В разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Внешние подключения** и нажмите .
2. Пропишите корневой сертификат на этапе установки шлюза удаленного доступа.

   После успешной настройки шлюза на аутентификацию по сертификату десктоп-клиент подключится к серверу через этот шлюз.

   Если сертификат устареет или окажется скомпрометированным, создайте новый, нажав .

Многофакторная аутентификация

Чтобы настроить многофакторную аутентификацию (MFA):

1. 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 по Kerberos нужно использовать MFA

при запуске десктоп-клиента и портала администрирования.

- **Многофакторная аутентификация при использовании имени пользователя и пароля**, если для аутентификации внутренних пользователей по имени и паролю нужно использовать MFA при запуске десктоп-клиента и портала администрирования.

3. В поле **Внешние пользователи** активируйте опцию **Многофакторная аутентификация при использовании имени пользователя и пароля**, если для аутентификации внешних пользователей по имени и паролю нужно использовать MFA при запуске десктоп-клиента и портала администрирования.
4. Нажмите **[Сохранить]**.

Далее настройте RADIUS-сервер.

Syslog/SIEM

Можно настроить переадресацию журнала в rsyslog-сервер.

Сведения о каждом событии в СТД «Термит» отправляются как отдельное rsyslog-сообщение. Текст rsyslog-сообщения соответствует информации о событии, отображающейся в веб-интерфейсе системы в разделе Журнал событий.

Чтобы настроить параметры для интеграции Syslog:

1. 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]**.

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. 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 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. 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. Нажмите **[Сохранить]**.

Данные об администраторе системы изменены.

Разблокировка учетной записи администратора системы

При неудачной авторизации в систему СТД «Термит» учетная запись блокируется. Подробнее смотрите в разделе Политика блокировки встроенных учетных записей.

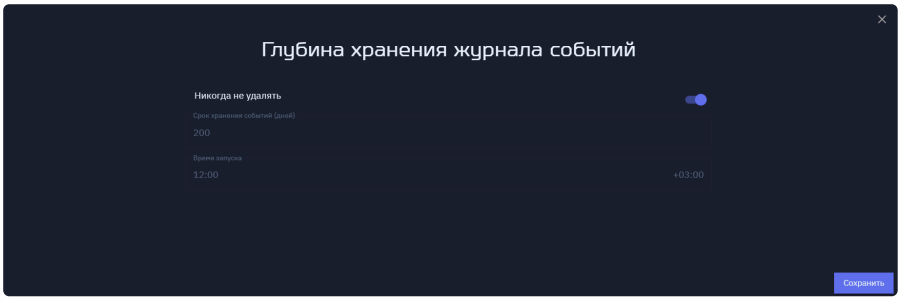
Для разблокировки учетной записи администратора системы в разделе **Настройки**, на вкладке **Общие настройки** наведите курсор на **Администратор системы** и нажмите на 🔓. Учетная запись разблокирована.

Глубина хранения журналов событий

В системе можно очищать старые записи журнала событий.

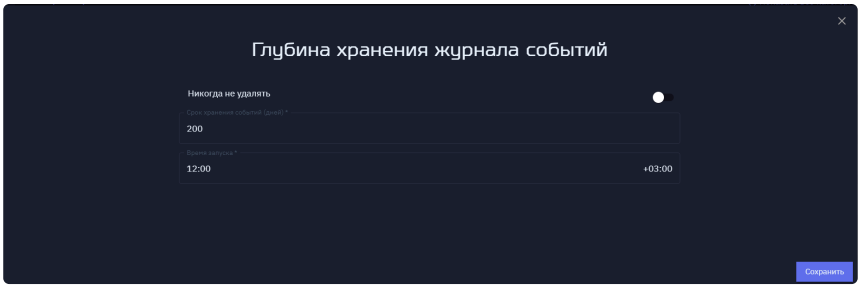
Чтобы настроить срок хранения записей:

1. 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 задайте:

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



3. Нажмите **[Сохранить]**.

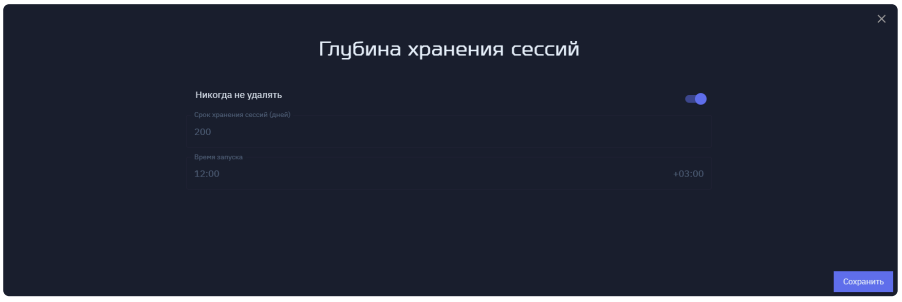
После очистки в журнале событий появится запись о статусе операции: сколько событий было удалено, дата самого старого и нового события.

Глубина хранения сессий

В системе можно очищать историю закрытых сессий пользователей.

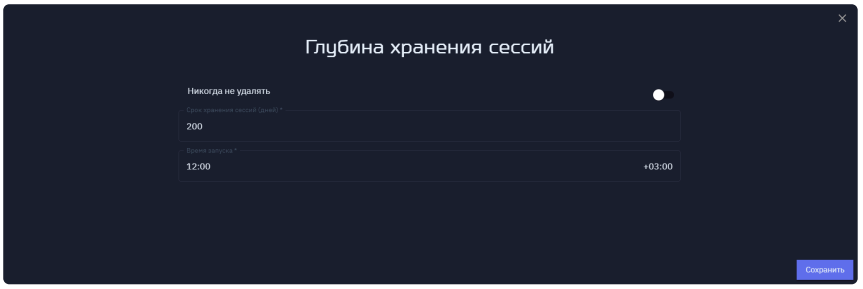
Чтобы настроить срок хранения:

1. 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. 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.
5. В параметре **Протокол аутентификации RADIUS** выберите протокол **PAP**, **CHAP** или **MSCHAPv2**.

6. Нажмите **[Сохранить]**.

RADIUS-сервер настроен.

Политика блокировки встроенных учетных записей

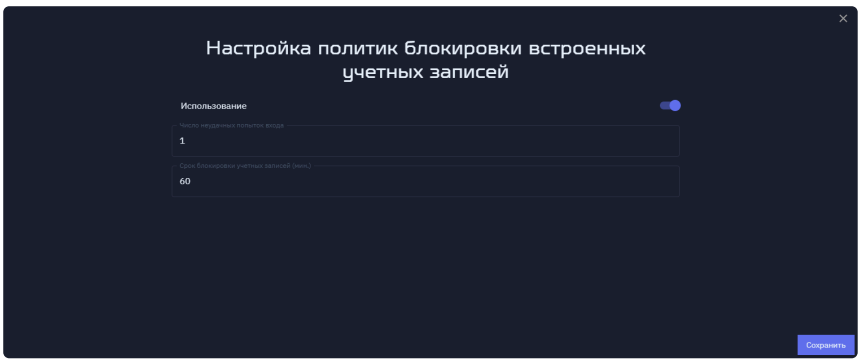
Политика блокировки встроенных учетных записей необходима для обеспечения безопасности системы и применяется только для локальной учетной записи «tadm». Учетная запись блокируется, если пользователь совершает несколько неудачных попыток входа в систему СТД «Термит». Это помогает предотвратить несанкционированный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

     За время блокировки злоумышленник не сможет подобрать пароль методом перебора или с помощью 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 задана.

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

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 в портале администратора, десктоп-клиенте и на терминальных серверах.

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).

Для работы пользователей с СТД «Термит» 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»:

Для работы пользователей с СТД «Термит» необходимо, чтобы система могла выполнять поиск пользователей в LDAP-каталоге, получать список групп, в которые входит пользователь, и т.д.

- 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 имя объекта, который находится в списке членов групп.
- 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 в портале администратора или десктоп-клиенте.
  - **Атрибут для аутентификации на терминальном сервере Linux** — в значении этого атрибута применяется имя, которое будет передаваться на сервер под управлением Linux.
  - **Атрибут для аутентификации на терминальном сервере Windows** — в значении этого атрибута применяется 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 СТД «Термит» 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 ;
- настроить Kerberos, нажав .
- изменить настройки LDAP-каталога, нажав .

Добавление LDAP-каталога

Чтобы добавить LDAP-каталог:

1. В левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и нажмите **[Добавить LDAP]**.
3. Задайте параметры для подключения службы каталогов:
   - **Полное имя каталога** — 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** — уникальное имя пользователя в LDAP-каталоге. Например, для домена example.com: «CN=termitsvc,CN=users,DC=example,DC=com».

  Посмотреть уникальное имя пользователя можно в зависимости от выбранной реализации LDAP следующими способами:

  ▸ AD

  ▸ Samba

  ▸ FreeIpa

- **Пароль** — пароль от сервисной учетной записи.
- **Период синхронизации (мин.)**

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

     Тип зависит от выбранной реализации LDAP:
     - Для Samba DC и Red ADM требуется выбрать тип каталога **AD**.
     - Для ALD Pro требуется выбрать тип каталога **FreeIPA**.
     - Для OpenLDAP и других реализаций LDAP-каталогов требуется выбрать тип **Другой**.

     ▸ **AD**

     ▸ **FreeIPA**

     ▸ **Другой (для OpenLDAP)**

6. Нажмите **[Далее]**.
7. Чтобы добавить адрес сервера LDAP, нажмите ＋.

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

8. 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.
9. Нажмите **Сохранить** > **Далее**.
10. На вкладке **Подтверждение информации** проверьте:
    - информацию о LDAP-сервере;
    - соединение. При успешном соединении появится сообщение «Проверка соединения прошла успешна».

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

Состояние синхронизации LDAP и системы смотрите в разделе Журнал событий.

Изменение настроек LDAP-каталога

Чтобы изменить настройки LDAP-каталога:

1. 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 каталога** — 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** — уникальное имя пользователя в LDAP-каталоге. Например, для домена example.com: «CN=termitsvc,CN=users,DC=example,DC=com».
   - **Пароль** — пароль от сервисной учетной записи.
   - **Период синхронизации (мин.)**.
6. Нажмите **[Далее]**.
7. Чтобы задать атрибуты используемого LDAP-каталога, укажите:
   - **Тип LDAP-каталога** — тип: **AD**, **FreeIPA** или **Другой**.

     Тип зависит от выбранной реализации LDAP:
     - Для Samba DC и Red ADM требуется выбрать тип каталога **AD**.
     - Для ALD Pro требуется выбрать тип каталога **FreeIPA**.
     - Для OpenLDAP и других реализаций LDAP-каталогов требуется выбрать тип **Другой**.

     ▸ **AD**

     ▸ **FreeIPA**

     ▸ **Другой (для OpenLDAP)**
8. Нажмите **[Далее]**.
9. На вкладке **Список LDAP-серверов**:

   ▸ **Можно добавить адрес сервера LDAP**

   ▸ **Можно изменить адрес сервера LDAP**

   ▸ **Можно удалить адрес сервера LDAP**

Удаление LDAP-каталога

Чтобы удалить LDAP-каталог:

1. В левом меню выберите раздел **Настройки**.
2. Перейдите на вкладку **LDAP-каталоги** и наведите курсор на полное имя каталога.
3. Нажмите 🗑.
4. Нажмите **[Да]**.

После удаления LDAP-каталога пользователи не смогут:

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

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.

Поддерживаются следующие подключения десктоп-клиента с терминальным сервером:

- десктоп-клиент на ОС Linux с терминальным сервером на ОС Linux;
- десктоп-клиент на ОС Windows с терминальным сервером на ОС Linux;
- десктоп-клиент на ОС Windows с терминальным сервером на ОС Windows.

Не поддерживаются подключения десктоп-клиента на ОС Linux с терминальным сервером на ОС Windows.

Создание keytab-файла

▸ AD

▸ FreeIPA/ALD Pro

Загрузка keytab-файла

Чтобы загрузить `keytab-файл`:

1. 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 загружен.

Настройка терминального сервера

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

- 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`.

- Перезагрузите sshd с помощью команды:

```
sudo systemctl restart sshd
```

Дополнительно для систем Astra Linux и ALT Linux

Для корректной обработки имён пользователей с заглавными буквами:

- В файле `/etc/sssd/sssd.conf` укажите:

```
case_sensitive = Preserving
```

- Перезагрузите sssd с помощью команды:

```
sudo systemctl restart sssd
```

Для серверов под управлением Windows настройка не требуется, аутентификация по Kerberos осуществляется по умолчанию через протоколы Windows.

Настройка десктоп-клиента

Перед началом настройки проверьте, что десктоп-клиент и терминальный сервер введены в один домен.

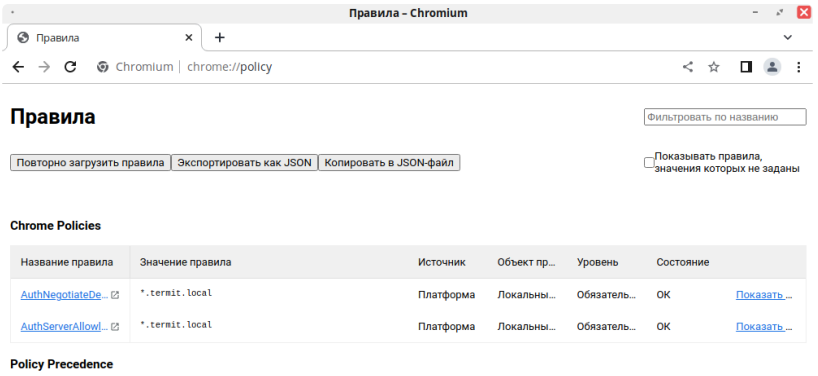
- Для использования Kerberos на клиентском устройстве с ОС Windows настройте систему. Для этого:
  1. В разделе **Конфигурация компьютера > Административные шаблоны > Система > Передача учетных данных** настройте политики «Разрешить передачу учетных данных, установленных по умолчанию» и «Разрешить передачу учетных данных, установленных по умолчанию, с проверкой подлинности сервера 'только NTLM'». Укажите в них SPN для терминальных серверов. Настройки должны выполняться администратором домена.

     Например:

     - TERMSRV/terminal1.example.com — для включения Kerberos при доступе на сервер terminal1.example.com.
     - TERMSRV/*.example.com — для включения Kerberos при доступе ко всем серверам из домена example.com.
  2. Добавьте адрес broker.example.com в доверенные сайты.
  3. Включите опцию «Автоматический вход с текущим именем пользователя и паролем» в параметрах безопасности доверенных сайтов.
  4. Перейдите в другой браузер, например Edge, и проверьте, что настройки применились.

     После успешной настройки авторизация в СТД «Термит» будет выполнена без запроса ввода имени пользователя и пароля.
- Для использования Kerberos на клиентском устройстве с ОС Linux настройте браузер. Ниже приведены инструкции по настройке для Google Chrome и Mozilla Firefox.
  - Для браузера Google 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:

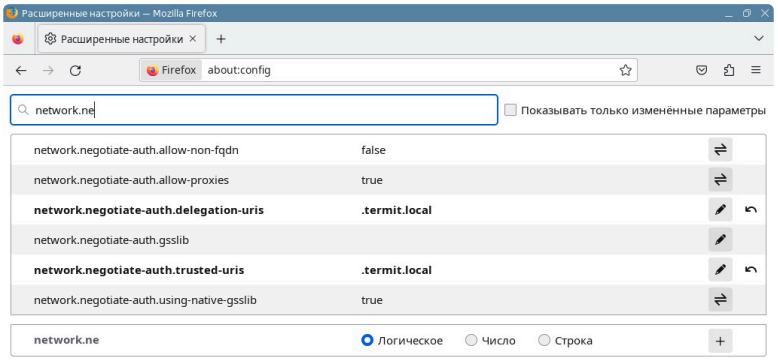
       ```
       BASH
       {
       "AuthServerAllowlist": "*.termit.local",
       "AuthNegotiateDelegateAllowlist": "*.termit.local"
       }
       ```
    2. Откройте в браузере Google Chrome страницу `chrome://policy` и проверьте, что настройки применились.



После успешной настройки авторизация в СТД «Термит» будет выполнена без запроса ввода имени пользователя и пароля.

- Для браузера Mozilla 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;



  3. Примените изменения и перезапустите браузер.

     После успешной настройки авторизация в СТД «Термит» будет выполнена без запроса ввода имени пользователя и пароля.

> При включенной аутентификации по Kerberos запрашивается пароль для открытия RDP-сессии с клиентской машины под управлением Linux.

Роли

На вкладке **Роли** можно настроить роли:

- **Администраторы**. Администраторы могут полностью контролировать систему, например, управлять серверами, пользователями и приложениями.
- **Служба поддержки**. Служба поддержки может просматривать настройки, информацию о серверах и сессиях в разделе **Обзор**, журнал событий, список сессий, завершать сессии и блокировать пользователей. Выполняет функцию L1 технической поддержки.
- **Пользователи**. У пользователей есть учетные записи, с помощью которых они имеют доступ к СТД «Термит». Только пользователи могут запускать приложения.
- **Аудитор ИБ**. Пользователям с ролью «Аудитор ИБ» предоставлены права на доступ в режиме «Только чтение», без возможности внесения изменений, к разделам: **Обзор**, **Группы серверов**, **Серверы**, **Приложения**, **Сессии**, **Журнал событий** и **Настройки**.

Настройка роли

Чтобы настроить роли:

1. В разделе **Настройки** перейдите на вкладку **Роли**.
2. Наведите курсор на **Администраторы** и нажмите ✎.
3. Нажмите ＋.

   При нажатии на ＋ необходимо добавлять группы пользователей из всех LDAP-каталогов, которые будут использоваться. После добавления в списке для каждой группы будет указано, к какому LDAP-каталогу она принадлежит.

4. Добавьте группы из каталога пользователей для роли администраторов. Можно добавить несколько групп. Также поддерживаются вложенные группы.
5. Нажмите **Сохранить** > **Сохранить**.

Для ролей **Служба поддержки**, **Пользователи** и **Аудитор ИБ** повторите действия из шагов 3-5.

Удаление группы пользователей

Чтобы удалить группу пользователей:

1. В разделе **Настройки** перейдите на вкладку **Роли**.
2. Наведите курсор на **Администраторы** и нажмите .
3. Наведите курсор на группу пользователей и нажмите .
4. Нажмите **[Да]**.
5. Нажмите **[Сохранить]**.

Группа пользователей удалена.

Для ролей **Служба поддержки**, **Пользователи** и **Аудитор ИБ** повторите действия из шагов 3-5.

Настройка профиля пользователя в терминальной среде Windows

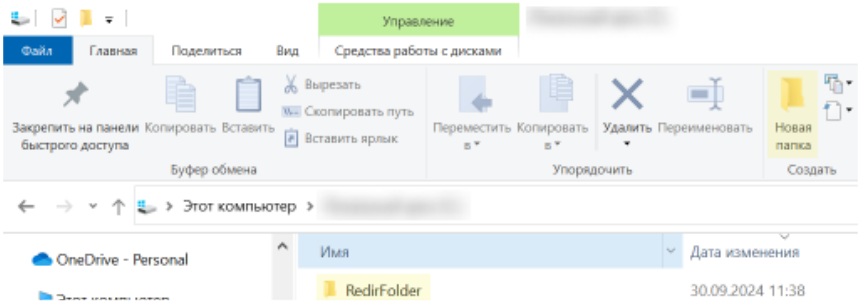
Перенаправление папок позволяет пользователям и администраторам вручную или с помощью групповой политики перенаправлять путь к определенной папке в новое расположение. Новым расположением может быть папка на терминальном сервере или каталог на файловом сервере. Пользователи будут работать с данными в перенаправленной папке.

В этом документе описано, как настроить перенаправления папок (folder redirection) на компьютерах пользователей в домене Active Directory (AD) с помощью групповых политик (GPO) для группы доступа пользователей домена.

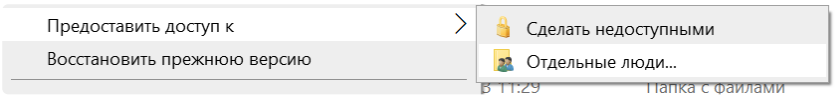
Групповая политика применяется к пользователю или компьютеру в зависимости от расположения объектов пользователя и компьютера в AD. В некоторых случаях пользователям могут потребоваться политики, применяемые на основе расположения как объекта пользователя, так и объекта компьютера, либо только расположения объекта компьютера. Для этого можно использовать функцию замыкания групповой политики (Loopback), чтобы применить объекты групповой политики (GPO).

Подробнее о Loopback можно прочесть на официальном сайте Microsoft.

1. Создайте в домене AD группу и добавьте в нее пользователей с помощью консоли Active Directory Users and Computers (ADUC).
2. Создайте и опубликуйте на файловом сервере сетевую папку, в которой будут храниться перенаправленные папки с помощью проводника Windows:
   a. На файловом сервере, где будет размещена общая папка, создайте новую папку и назовите ее, например «RedirFolder».



   b. Нажмите правой кнопкой мыши по папке, разверните **Предоставить доступ к (Give Access to)** и выберите **Отдельные люди (Specific people)**.



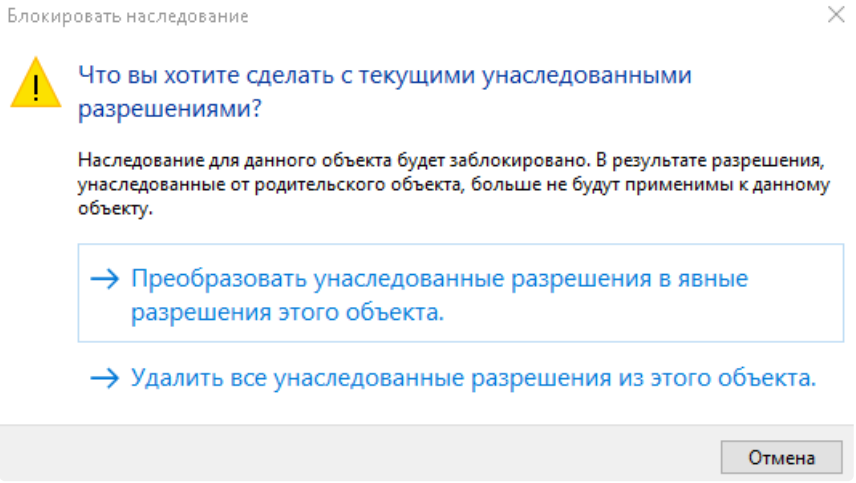
c. Предоставьте полный доступ (чтение/запись) для **Authenticated users** .

d. Нажмите **Поделиться > Готово** (**Share > Done**).

3. Для того чтобы обеспечить каждому пользователю доступ только к его файлам, необходимо настроить правильные разрешения NTFS для папки:

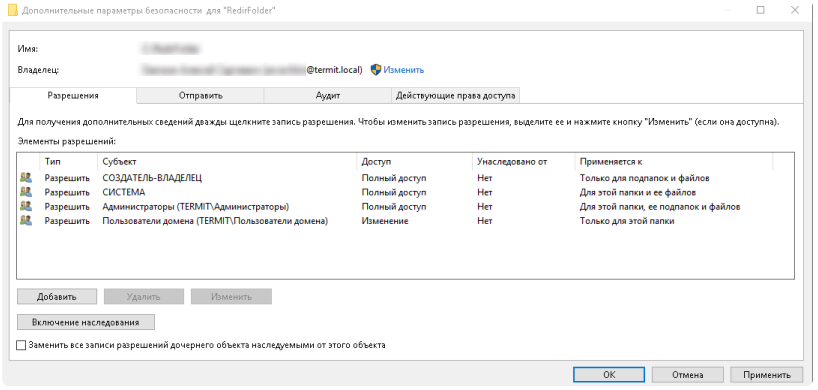
   a. В свойствах папки перейдите на вкладку **Безопасность (Security)**, нажмите **[Дополнительно]** (**[Advanced]**), затем нажмите **[Отключение наследования]** (**[Disable Inheritance]**).

   b. В открывшемся окне выберите **Преобразовать унаследованные разрешения в явные разрешения этого объекта (Convert inherited permissions into explicit permissions on the object)**.



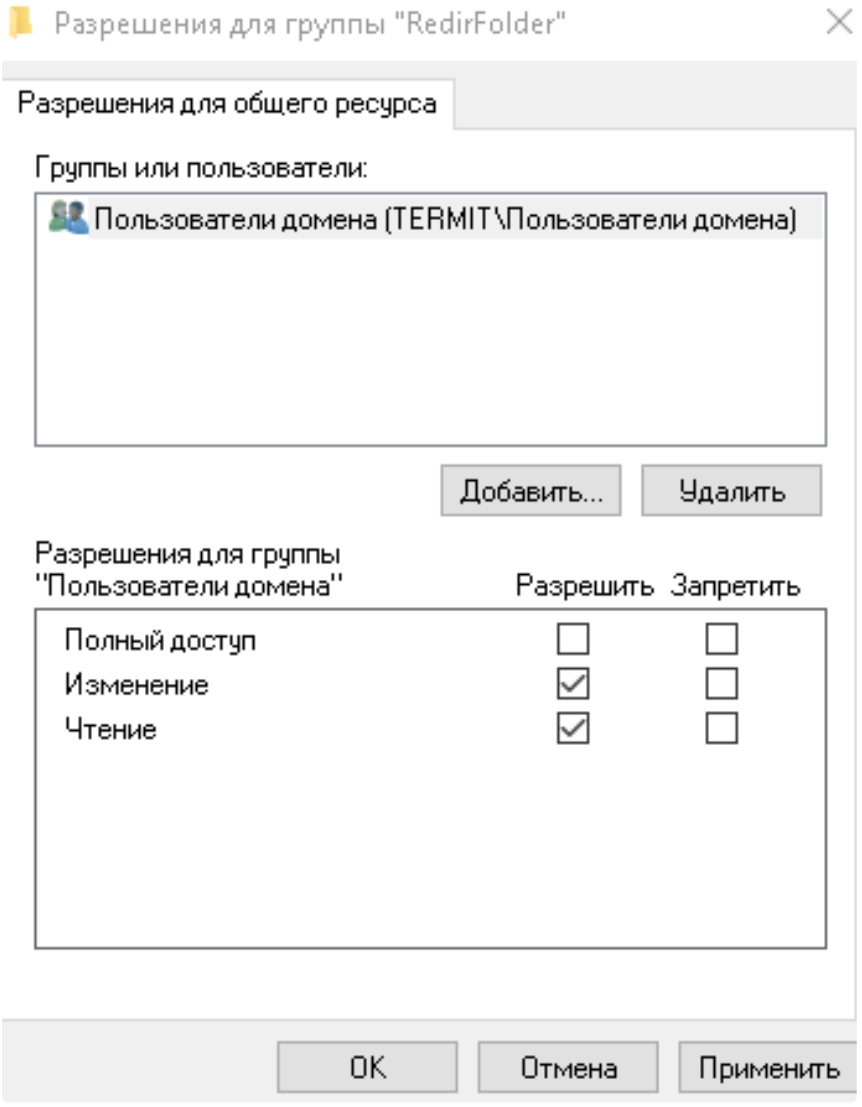
   c. В списке разрешений NTFS оставьте права:

   - СОЗДАТЕЛЬ-ВЛАДЕЛЕЦ (Полный доступ, Только для подпапок и файлов) (CREATOR OWNER (Full control, Subfolders and files only))
   - 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))
   - Пользователи домена (Изменение, Чтение и выполнение, Запись, Только для этой папки) (Domain users (Modify, Read & execute, Write, This folder))



d. На файловом сервере в свойствах сетевой папки перейдите на вкладку **Доступ (Sharing)**, нажмите **Расширенная настройка > Разрешения** (**Advanced Sharing: > Permissions**) и активируйте опцию **Полный доступ (Full Control)**.

   После настройки разрешения пользователи смогут создавать папки в каталоге, а доступ к содержимому вложенных папок будет только у владельцев-пользователей.



4. Создайте в домене групповую политику перенаправления папок для пользователей. Для этого:

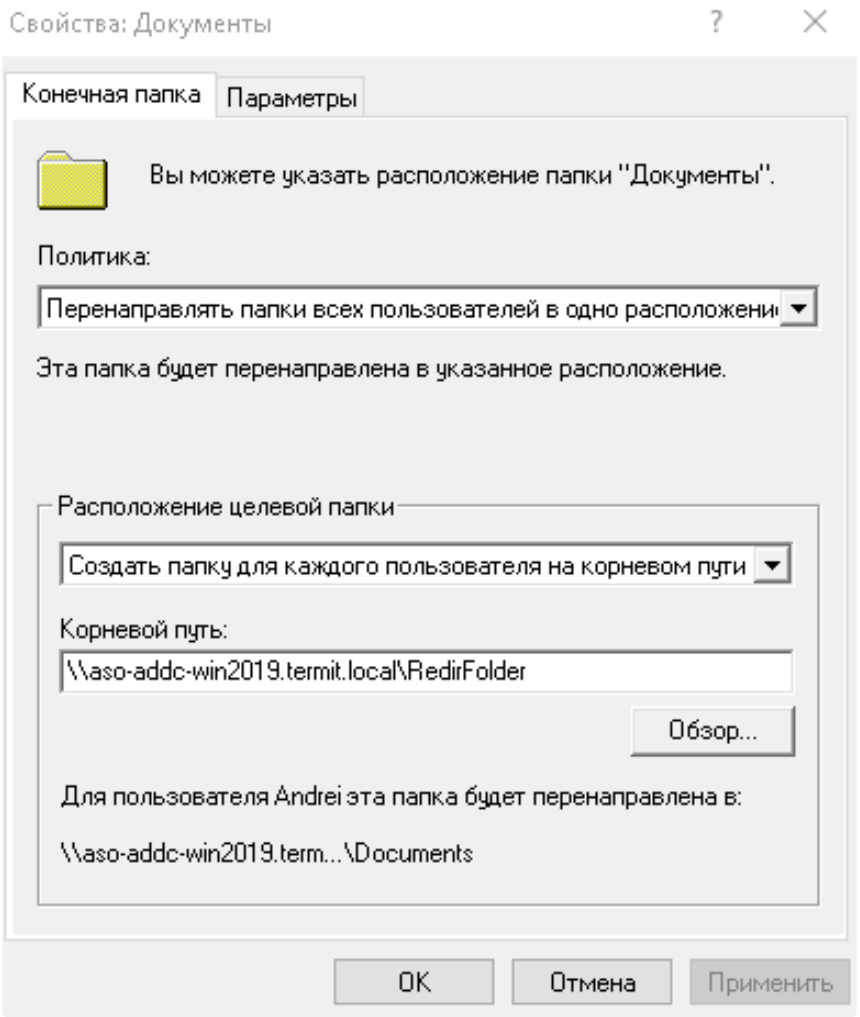
   a. Запустите консоль управления групповой политикой (GPMC).

   b. Создайте новую GPO и назначьте на Organizational Unit с пользователями.

5. В редакторе управления групповыми политиками разверните **Конфигурация пользователя > Политики > Конфигурация Windows > Перенаправление папки** (**User Configuration > Policies > Windows Settings > Folder Redirection**.

> В разделе **Перенаправление папки (Folder Redirection)** находятся опции для перенаправления различных папок профиля пользователя. В этом примере приведена настройка перенаправления только для папки `Документы (Documents)`. Остальные папки можно настроить таким же образом.

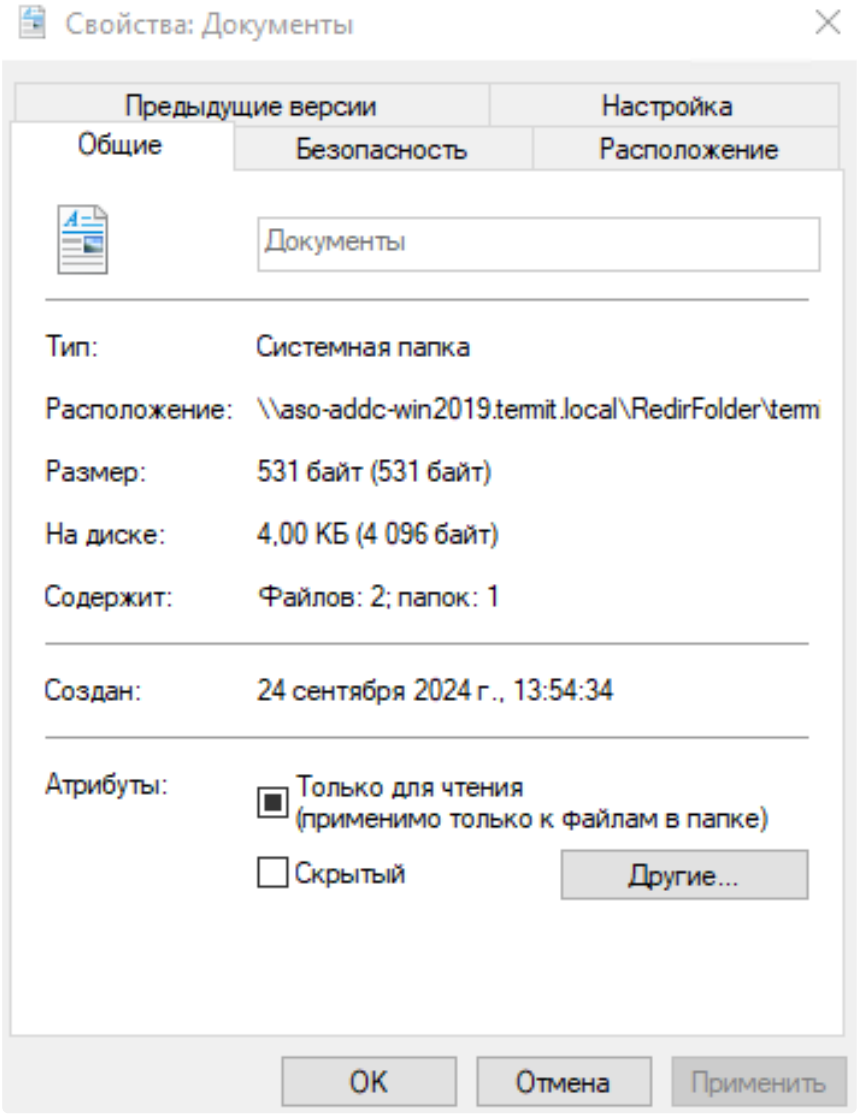
6. Откройте свойства `Документы (Documents)` и на вкладке **Корневая папка (Target)** укажите следующие параметры перенаправления каталога:
   - **Политика (Settings)** – Перенаправлять папки всех пользователей в одно расположение (Basic, Redirect everyone's folder to the same location);
   - **Расположение целевой папки (Target folder location)** – Создать папку для каждого пользователя на корневом пути (Create a folder for each user under the root path);
   - **Корневой путь (Root path)** – \\asso-addc-win2019.termit.local\RedirFolder.



Добавьте адрес файлового сервера и/или домен в список доверенных зон, используя групповую политику **Список назначений зоны для веб-сайтов (GPO Site to Zone Assignment List)** в **Конфигурация компьютера > Административные шаблоны > Компоненты Windows > Internet Explorer > Панель управления Интернетом > Страница безопасности** (в **Computer Configuration > Administrative Templates > Windows Components > Internet Explorer > Internet Control Panel > Security Page**).

Иначе при запуске ярлыков и исполняемых файлов из перенаправленного каталога могут появляться предупреждения системы безопасности Windows.

7. Проверьте работу групповой политики перенаправления папки. Для этого:
   a. Запустите **десктоп-клиент Termit > рабочий стол**.
   b. Откройте свойства папки `Документы (Documents)` и убедитесь, что в параметре **Расположение (Location)** указан UNC-путь к вашему файловому серверу.



Вы можете создавать файлы и папки в `Документы (Documents)`. И они будут доступны пользователю с любого компьютера в вашем домене.