Linux

- SSH-доступ к серверу Timeweb Cloud по ключу

SSH-доступ к серверу Timeweb Cloud по ключу

Эта инструкция описывает, как создать SSH-ключ на локальном компьютере, добавить публичный ключ в Timeweb Cloud и проверить подключение к серверу без использования пароля.

> **Важно:** во всех примерах ниже используется тестовый IP-адрес `203.0.113.10`.
> Это адрес только для примера. Перед выполнением команд замените `203.0.113.10` на **реальный IP-адрес вашего сервера в Timeweb Cloud**.

После настройки команда:

```
ssh root@203.0.113.10
```

должна подключать к серверу с использованием локального SSH-ключа.

> **Никогда не передавайте приватный SSH-ключ другим людям или сервисам.**
> В Timeweb Cloud добавляется только публичная часть ключа.

---

1. Проверить, есть ли SSH-ключ на компьютере

Windows

Откройте **PowerShell** и выполните:

```
Get-ChildItem ~/.ssh
```

Если среди файлов есть, например:

```
id_ed25519
id_ed25519.pub
```

значит SSH-ключ уже создан.

Файл:

```
id_ed25519
```

— это **приватный ключ**.

Его нельзя передавать другим людям, агентам, сайтам или сервисам.

Файл:

```
id_ed25519.pub
```

— это **публичный ключ**.

Именно его можно добавлять в Timeweb Cloud.

Если таких файлов нет — создайте новый ключ.

---

2. Создать SSH-ключ

В PowerShell выполните:

```
ssh-keygen -t ed25519 -C "timeweb"
```

Появится запрос:

```
Enter file in which to save the key
```

Если отдельный путь не нужен, просто нажмите:

```
Enter
```

В Windows ключ обычно будет сохранён в:

```
C:\Users\ИМЯ_ПОЛЬЗОВАТЕЛЯ\.ssh\id_ed25519
```

После этого появится запрос:

```
Enter passphrase
```

Можно установить пароль на SSH-ключ для дополнительной защиты.

Если пароль не нужен, дважды нажмите `Enter`.

После создания появятся два файла:

```
id_ed25519
id_ed25519.pub
```

---

3. Скопировать публичный SSH-ключ

Чтобы посмотреть публичный ключ, выполните:

```
Get-Content ~/.ssh/id_ed25519.pub
```

Вы увидите строку примерно такого вида:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI..................... timeweb
```

Нужно скопировать **всю строку целиком**.

Удобнее сразу скопировать ключ в буфер обмена:

```
Get-Content ~/.ssh/id_ed25519.pub | Set-Clipboard
```

Теперь публичный ключ можно вставить в Timeweb Cloud.

---

4. Добавить SSH-ключ в Timeweb Cloud

Откройте:

Timeweb Cloud → SSH-ключи

Нажмите:

Добавить ключ

В поле **Ключ** вставьте содержимое файла:

```
id_ed25519.pub
```

Например:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI..................... timeweb
```

В поле **Название ключа** укажите понятное название компьютера.

Например:

```
Work-PC
```

или:

```
Office-PC
```

или:

```
Windows-PC-2026
```

После этого нажмите:

Добавить.

> **Важно:** не вставляйте в Timeweb содержимое файла `id_ed25519`.
> Это приватный ключ.

> Добавлять необходимо только файл с расширением `.pub`.

---

5. Добавить ключ на сервер

Есть два основных варианта.

Вариант 1. Создаётся новый сервер

Если сервер только создаётся, выберите созданный SSH-ключ при настройке сервера в Timeweb Cloud.

Timeweb автоматически добавит публичный ключ на сервер.

После создания сервера можно проверить подключение:

```
ssh root@203.0.113.10
```

> Замените `203.0.113.10` на реальный IP-адрес созданного сервера.

Вариант 2. Сервер уже существует

Если сервер был создан ранее, простого добавления ключа в общий раздел **SSH-ключи** может быть недостаточно.

Публичный ключ должен присутствовать непосредственно на сервере в файле:

```
/root/.ssh/authorized_keys
```

Сначала подключитесь к серверу по существующему паролю:

```
ssh root@203.0.113.10
```

> Вместо `203.0.113.10` укажите реальный IP вашего сервера.

После входа выполните:

```
mkdir -p ~/.ssh
chmod 700 ~/.ssh
nano ~/.ssh/authorized_keys
```

Вставьте в файл ваш публичный ключ:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI..................... timeweb
```

Сохраните файл.

Для редактора `nano`:

```
Ctrl + O
Enter
Ctrl + X
```

Затем выполните:

```
chmod 600 ~/.ssh/authorized_keys
```

---

6. Проверить подключение по SSH

На локальном компьютере откройте PowerShell и выполните:

```
ssh root@203.0.113.10
```

> **Не забудьте заменить `203.0.113.10` на реальный IP-адрес сервера Timeweb Cloud.**

При первом подключении может появиться сообщение:

```
Are you sure you want to continue connecting (yes/no/[fingerprint])?
```

Введите:

```
yes
```

Если всё настроено правильно, откроется консоль сервера.

Например:

```
root@server:~#
```

Это означает, что SSH-доступ работает.

---

7. Если SSH не использует нужный ключ

Можно явно указать путь к приватному ключу:

```
ssh -i ~/.ssh/id_ed25519 root@203.0.113.10
```

Где:

```
203.0.113.10
```

необходимо заменить на реальный IP вашего сервера.

Для диагностики подключения можно использовать подробный режим:

```
ssh -v root@203.0.113.10
```

В выводе можно искать строки:

```
Offering public key
```

и:

```
Server accepts key
```

Они указывают на то, что SSH-клиент предлагает ключ серверу и сервер его принимает.

8. Проверить сервер перед передачей задачи AI-агенту

Перед тем как поручать агенту установку или настройку программ на сервере, самостоятельно убедитесь, что SSH-доступ работает.

Выполните:

```
ssh root@203.0.113.10
```

> Вместо `203.0.113.10` подставьте реальный IP сервера.

После подключения полезно проверить, что уже работает на сервере.

Проверить Docker-контейнеры

```
docker ps
```

Если Docker не установлен, команда может вернуть ошибку — это нормально.

Проверить занятые сетевые порты

```
ss -tulpn
```

Особенно важно проверить порты:

```
80
443
```

Порт `80` обычно используется для HTTP.

Порт `443` обычно используется для HTTPS.

> **Важно:** если на сервере уже работает сайт, Nginx, Apache, Docker, reverse proxy, VPN или другой сервис, обязательно сообщите об этом агенту.
>
> Нельзя считать сервер «чистым» и без проверки изменять или удалять существующие сервисы, особенно использующие порты `80` и `443`.

Быстрая памятка

Создать SSH-ключ

```
ssh-keygen -t ed25519 -C "timeweb"
```

Скопировать публичный ключ

```
Get-Content ~/.ssh/id_ed25519.pub | Set-Clipboard
```

Добавить ключ

Открыть:

Timeweb Cloud → SSH-ключи → Добавить ключ

и вставить содержимое:

```
id_ed25519.pub
```

Проверить подключение

```
ssh root@203.0.113.10
```

Перед выполнением заменить:

```
203.0.113.10
```

на:

```
РЕАЛЬНЫЙ_IP_СЕРВЕРА
```

Например, если Timeweb показывает IP:

```
192.0.2.25
```

то команда будет выглядеть так:

```
ssh root@192.0.2.25
```

Явно указать SSH-ключ

```
ssh -i ~/.ssh/id_ed25519 root@203.0.113.10
```

Здесь также необходимо заменить IP на реальный.

Что можно и нельзя передавать

✅ Можно передавать

Публичный ключ:

```
~/.ssh/id_ed25519.pub
```

Он выглядит примерно так:

```
ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI..... timeweb
```

❌ Нельзя передавать

Приватный ключ:

```
~/.ssh/id_ed25519
```

Приватный ключ должен оставаться только на вашем компьютере.

> **Простое правило:**
> файл с `.pub` — публичный, его можно передавать.
> файл без `.pub` — приватный, его передавать нельзя.

Да, это стоит добавить обязательно. Лучше сначала проверить содержимое `~/.ssh`, чтобы случайно не перезаписать существующий ключ.

Вот улучшенный фрагмент для вставки в инструкцию:

Перенос SSH-ключа из Windows в WSL

Если SSH-ключ уже создан в Windows и настроен для доступа к серверу, новый ключ создавать не нужно. Его можно скопировать в WSL.

Допустим, ключ в Windows находится здесь:

```
C:\Users\evgeny\.ssh\id_ed25519
C:\Users\evgeny\.ssh\id_ed25519.pub
```

Сначала проверьте, нет ли в WSL файлов с такими же именами:

```
ls -la ~/.ssh
```

Или точечно:

```
ls -l ~/.ssh/id_ed25519 ~/.ssh/id_ed25519.pub
```

Если файлов нет, можно копировать.

Если они уже существуют, **не копируйте поверх них**, пока не убедитесь, что это тот же ключ. Лучше либо сохранить существующие файлы под другим именем, либо скопировать Windows-ключ в WSL с новым именем, например:

```
cp /mnt/c/Users/evgeny/.ssh/id_ed25519 ~/.ssh/timeweb_id_ed25519
cp /mnt/c/Users/evgeny/.ssh/id_ed25519.pub ~/.ssh/timeweb_id_ed25519.pub
```

Если файлов с такими именами в WSL нет, можно использовать стандартные имена:

```
cp /mnt/c/Users/evgeny/.ssh/id_ed25519 ~/.ssh/
cp /mnt/c/Users/evgeny/.ssh/id_ed25519.pub ~/.ssh/
```

После копирования обязательно выставьте правильные права:

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/id_ed25519
chmod 644 ~/.ssh/id_ed25519.pub
```

Если ключ был скопирован под другим именем:

```
chmod 600 ~/.ssh/timeweb_id_ed25519
chmod 644 ~/.ssh/timeweb_id_ed25519.pub
```

Проверить права:

```
ls -la ~/.ssh
```

Для приватного ключа права должны выглядеть примерно так:

```
-rw------- 1 user user ... id_ed25519
```

После этого можно проверить подключение:

```
ssh root@203.0.113.10
```

где `203.0.113.10` нужно заменить на реальный IP-адрес сервера.

Если ключ сохранён под нестандартным именем:

```
ssh -i ~/.ssh/timeweb_id_ed25519 root@203.0.113.10
```

> Используйте `cp`, а не `mv`, чтобы исходный ключ остался в Windows.
>
> Перед копированием всегда проверяйте `~/.ssh`, чтобы случайно не затереть уже существующий приватный ключ.