

1809 и более поздние) или Windows Server 2019 с установленным клиентом OpenSSH к таким устройствам с установленным сервером OpenSSH.

### 📌 Важно!

Если вы скачали OpenSSH из репозитория GitHub по адресу [PowerShell/openssh-portable](#), следуйте приведенным в репозитории инструкциям, а не инструкциям в этой статье.

## Установка OpenSSH с помощью приложения "Параметры" в Windows

Оба компонента OpenSSH можно установить с помощью "Параметров" Windows на устройствах Windows Server 2019 и Windows 10.

Чтобы установить компоненты OpenSSH, сделайте следующее:

1. Откройте приложение **Параметры**, выберите элементы **Приложения > Приложения и возможности**, щелкните **Дополнительные возможности**.
2. Просмотрите этот список и определите, установлено ли средство OpenSSH. Если нет, выберите пункт **Добавить компонент** в верхней части страницы и сделайте следующее:
  - Найдите **Клиент OpenSSH** и щелкните **Установить**.
  - Найдите **Сервер OpenSSH** и щелкните **Установить**.

После завершения установки вернитесь в раздел **Приложения > Приложения и возможности** и **Дополнительные возможности**, где теперь должно появиться средство OpenSSH.


### 📌 Примечание

При установке серверного компонента OpenSSH будет создано и включено правило брандмауэра с именем `openssh-server-in-tcp`. Правило разрешает входящий трафик SSH через порт 22. Если это правило не включено и этот порт не открыт, подключения будут отклонены или сброшены.


## Установка OpenSSH с помощью PowerShell

Чтобы установить OpenSSH с помощью PowerShell, запустите PowerShell от имени администратора и выполните следующие команды: [https://docs.microsoft.com/ru-ru/windows-server/administration/openssh/openssh\\_install\\_firstuse](https://docs.microsoft.com/ru-ru/windows-server/administration/openssh/openssh_install_firstuse)


Чтобы установить OpenSSH с помощью PowerShell, запустите PowerShell от имени администратора. Для проверки доступности OpenSSH выполните следующий командлет:

PowerShell	 Копировать
<pre>Get-WindowsCapability -Online   Where-Object Name -like 'OpenSSH*'</pre>	


Если ни один из них не установлен, должно отобразиться следующее:

	 Копировать
<pre>Name : OpenSSH.Client~~~~0.0.1.0 State : NotPresent  Name : OpenSSH.Server~~~~0.0.1.0 State : NotPresent</pre>	

Затем установите нужный серверный или клиентский компонент:


PowerShell	 Копировать
<pre># Install the OpenSSH Client Add-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0  # Install the OpenSSH Server Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0</pre>	

Оба командлета должны вернуть такие выходные данные:

	 Копировать
<pre>Path          : Online        : True RestartNeeded : False</pre>	

## Запуск и настройка OpenSSH Server

Чтобы запустить и настроить OpenSSH Server для первого использования, откройте PowerShell от имени администратора и выполните следующие команды для запуска `sshd service`:

PowerShell	 Копировать
------------	--


```
# Start the sshd service
Start-Service sshd

# OPTIONAL but recommended:
Set-Service -Name sshd -StartupType 'Automatic'


# Confirm the Firewall rule is configured. It should be created
automatically by setup. Run the following to verify
if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction
SilentlyContinue | Select-Object Name, Enabled)) {
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not
exist, creating it..."
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName
'OpenSSH Server (sshd)' -Enabled True -Direction Inbound -Protocol
TCP -Action Allow -LocalPort 22
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been
created and exists."
}
```

## Подключение к OpenSSH Server

После установки вы можете подключиться к серверу OpenSSH с устройства Windows 10 или Windows Server 2019, на котором установлен клиент OpenSSH, с помощью PowerShell, как показано ниже. Обязательно запустите PowerShell от имени администратора:

PowerShell	 Копировать
ssh username@servername	

Когда подключение будет установлено, отобразится примерно следующее сообщение:

	 Копировать
The authenticity of host 'servername (10.00.00.001)' can't be established. ECDSA key fingerprint is SHA256:(<a large string>). Are you sure you want to continue connecting (yes/no)?	

Если выбрать **Да**, этот сервер будет добавлен в список известных узлов SSH в клиенте Windows.

На этом этапе нужно ввести пароль. В целях безопасности пароль не будет

отображаться по мере ввода.

После подключения вы увидите командную оболочку Windows:

	Копировать
domain\username@SERVERNAME C:\Users\username>	

## Удаление OpenSSH с помощью приложения "Параметры" в Windows

Чтобы удалить OpenSSH с помощью приложения "Параметры" в Windows, сделайте следующее:

1. Откройте приложение **Параметры**, а затем выберите **Приложения > Приложения и возможности**.
2. Откройте страницу **Дополнительные возможности**.
3. В списке выберите компонент **Клиент OpenSSH** или **Сервер OpenSSH**.
4. Выберите **Удалить**.

## Удаление OpenSSH с помощью PowerShell

Чтобы удалить компоненты OpenSSH с помощью PowerShell, выполните следующие команды:

PowerShell	Копировать
<pre># Uninstall the OpenSSH Client Remove-WindowsCapability -Online -Name OpenSSH.Client~~~~0.0.1.0  # Uninstall the OpenSSH Server Remove-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0</pre>	

Если служба использовалась во время удаления, может потребоваться перезагрузка Windows.

## Рекомендуемое содержимое

### [Конфигурация сервера OpenSSH для Windows](#)

Сведения о конфигурации сервера OpenSSH для Windows 10 1809 и Windows Server 2019

## Управление ключами OpenSSH для Windows

Управление ключами OpenSSH для Windows с помощью средств Windows или PowerShell.

## Общие сведения об OpenSSH для Windows

Общие сведения о средствах OpenSSH, используемых администраторами Linux и других систем, кроме Windows, для кроссплатформенного управления удаленными системами.

## SSH в Терминале Windows

В этом руководстве описано, как настроить SSH-подключение в Терминале Windows.

## Подключение с помощью SSH

Подключение на устройство с ОС фабрики с помощью SSH

## Выполнение команды SSH

В этой статье описываются функции выполнения действия команды SSH.

## Команды Netsh для порта прокси-сервера интерфейса

Используйте команды порта прокси-сервера интерфейса Netsh, чтобы действовать в качестве прокси-серверов в сетях IPv4, IPv6 и приложениях.

Показать больше 

