


Get started with OpenSSH for Windows

Article • 08/05/2022 • 4 minutes to read

Applies to: Windows Server 2022, Windows Server 2019, Windows 10 (build 1809 and later)

OpenSSH is a connectivity tool for remote sign-in that uses the SSH protocol. It encrypts all traffic between client and server to eliminate eavesdropping, connection hijacking, and other attacks.

An OpenSSH-compatible client can be used to connect to Windows Server and Windows client devices.

 **Important**

If you downloaded the OpenSSH beta from the GitHub repo at [PowerShell/Win32-OpenSSH](#), follow the instructions listed there, not the ones in this article. Some information in the Win32-OpenSSH repository relates to prerelease product that may be substantially modified before it's released. Microsoft makes no warranties, express or implied, with respect to the information provided there.

Prerequisites

Before you start, your computer must meet the following requirements:

- A device running at least Windows Server 2019 or Windows 10 (build 1809).
- PowerShell 5.1 or later.
- An account that is a member of the built-in Administrators group.

Prerequisites check

To validate your environment, open an elevated PowerShell session and do the following:

- Type *winver.exe* and press enter to see the version details for your Windows device.
- Run `$PSVersionTable.PSVersion`. Verify your major version is at least 5, and your minor version at least 1. Learn more about [installing PowerShell on Windows](#).
- Run the command below. The output will show `True` when you're a member of the built-in Administrators group.

PowerShell

```
(New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())).IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)
```

Install OpenSSH for Windows

PowerShell

To install OpenSSH using PowerShell, run PowerShell as an Administrator. To make sure that OpenSSH is available, run the following cmdlet:

PowerShell

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH*'
```

The command should return the following output if neither are already installed:

Output

```
Name : OpenSSH.Client~~~~0.0.1.0
```

```
State : NotPresent

Name : OpenSSH.Server~~~~0.0.1.0
State : NotPresent
```

Then, install the server or client components as needed:

```
PowerShell

# 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
```

Both commands should return the following output:

```
Output

Path      :
Online    : True
RestartNeeded : False
```

To start and configure OpenSSH Server for initial use, open an elevated PowerShell prompt (right click, Run as an administrator), then run the following commands to start the `sshd service`:

```
PowerShell

# 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."
}
```

Connect to OpenSSH Server

Once installed, you can connect to OpenSSH Server from a Windows or Windows Server device with the OpenSSH client installed. From a PowerShell prompt, run the following command.

```
PowerShell

ssh domain\username@servername
```

Once connected, you get a message similar to the following output.

```
Output

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)?
```

Entering yes adds that server to the list of known SSH hosts on your Windows client.

At this point, you'll be prompted for your password. As a security precaution, your password won't be displayed as you type.

Once connected, you'll see the Windows command shell prompt:

```
Output

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

Uninstall OpenSSH for Windows

PowerShell

To uninstall the OpenSSH components using PowerShell, use the following commands:

PowerShell

```
# 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
```

You may need to restart Windows afterwards if the service was in use at the time it was uninstalled.

Next steps

Now that you've installed OpenSSH Server for Windows, here are some articles that might help you as you use it:

- Learn more about using key pairs for authentication in [OpenSSH key management](#)
- Learn more about the [OpenSSH Server configuration for Windows](#)