Get started with OpenSSH for Windows

Article • 11/01/2024 • 23 contributors •

Applies to: Windows Server 2025, Windows Server 2022, Windows Server 2019, Windows Server 2016

Feedback

Choose your product version:

Windows Server 2025 | Windows Server 2022 | Windows Server 2019

In this article

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:

- Enter *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 following command. The output shows `True` when you're a member of the built-in Administrators group.

```
PowerShell                                                    Copy

(New-Object Security.Principal.WindowsPrincipal([Security.Principal.Windows
```

Enable OpenSSH for Windows Server 2025

Starting with Windows Server 2025, OpenSSH is now installed by default. You can also enable or disable the `sshd` service in Server Manager.

GUI | PowerShell

To enable SSHD using PowerShell:

1. Open PowerShell as an administrator and run the following cmdlet to start the SSHD service:

```
PowerShell                                                    Copy

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

2. You can also run the following optional but recommended cmdlet to automatically start SSHD to make sure it stays enabled:

```
PowerShell                                                    Copy

Set-Service -Name sshd -StartupType 'Automatic'
```

3. Finally, run the following command to verify that the SSHD setup process automatically configured the firewall rule:

```
PowerShell                                                    Copy

if (!(Get-NetFirewallRule -Name "OpenSSH-Server-In-TCP" -ErrorAction Si
    Write-Output "Firewall Rule 'OpenSSH-Server-In-TCP' does not exist,
    New-NetFirewallRule -Name 'OpenSSH-Server-In-TCP' -DisplayName 'Ope
} else {
    Write-Output "Firewall rule 'OpenSSH-Server-In-TCP' has been create
}
```

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                                                    Copy

ssh domain\username@servername
```

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

PowerShell Copy

```
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, the service prompts you for your password. As a security precaution, the characters of your password aren't displayed as you enter them.

Once connected, you should see the following Windows command shell prompt:

PowerShell Copy

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

Uninstall OpenSSH for Windows

GUI | PowerShell

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

PowerShell Copy

```
# 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
```

If the service was in use when you uninstalled it, you should restart Windows.

Next steps

Now that you're done installing OpenSSH Server for Windows, here are some articles that can help you learn how to use it:

- Learn more about using key pairs for authentication in OpenSSH key management
- Learn more about the OpenSSH Server configuration for Windows

Feedback

Was this page helpful? Yes No

Additional resources

Training

Module
Develop on a remote machine using SSH with Visual Studio Code - Training

In this module, you'll learn how to seamlessly develop on a remote machine using the Visual Studio Code Remote - SSH extension. We'll explore how to run and debug code located on a remote machine, while locally using Visual Studio Code's full feature set.

Certification
Microsoft Certified: Windows Server Hybrid Administrator Associate - Certifications

As a Windows Server hybrid administrator, you integrate Windows Server environments with Azure services and manage Windows Server in on-premises networks.

English (United States) Your Privacy Choices Theme

Manage cookies Previous Versions Blog Contribute Privacy Terms of Use Trademarks © Microsoft 2024