



# wolfSSH Embedded SSH Library

Current Version: 1.1.0  
Release Date: 06/16/2017

## Description

The wolfSSH library is a lightweight SSHv2 server library written in ANSI C and targeted for embedded, RTOS, and resource-constrained environments - primarily because of its small size, speed, and feature set. It is commonly used in standard operating environments as well because of its royalty-free pricing and excellent cross platform support. wolfSSL supports the industry standard **SSH v2** and offers progressive ciphers such as Poly1305, ChaCha20, NTRU, and SHA-3.

wolfSSH is powered by the wolfCrypt library. wolfCrypt is **FIPS 140-2 Level 1 validated**, with certificate #2425. For additional information, visit our FIPS FAQ page or contact [fips@wolfssl.com](mailto:fips@wolfssl.com)

wolfSSH is built for maximum portability, and is generally very easy to compile on new platforms. If your desired platform is not listed under the supported operating environments, please contact wolfSSL Inc.

wolfSSH supports the C programming language as a primary interface. If you have interest in using wolfSSH in another programming language that it does not currently support, please contact wolfSSL Inc. at [info@wolfssl.com](mailto:info@wolfssl.com).

## Features

- SSH v2.0 (server)
- Minimum size of 33kb
- Runtime memory usage between 1.4 and 2kb, not including a configurable receive buffer
- Multiple Hashing Functions:  
SHA-1, SHA-2 (SHA-256, SHA-384, SHA-512), BLAKE2b, Poly1305
- Block and Stream Ciphers:  
AES (CBC, CTR, GCM, CCM), Camellia, ChaCha20
- Public Key Options:  
RSA, DH, EDH, NTRU
- ECC Support  
ECDH, ECDSA, ECDHE
- Curve25519 and Ed25519
- Client authentication support (RSA key, password)
- Simple API
- PEM and DER certificate support
- Hardware crypto support  
AES-NI, Cavium, STM32, Kinetis, PIC32, Intel AVX1/2
- much more...

---

## Supported Chipmakers

wolfSSH has support for chipsets including ARM, Intel, Motorola, mbed, Freescale, Microchip (PIC32), ST (STM32F2/F4), NXP, Analog Devices, TI, and more.

- If you would like to use or test wolfSSH on another chipset, let us know and we'll be happy to support you.

## Supported Operating Environments

Win32/64, Linux, Mac OS X, Solaris, ThreadX, VxWorks, FreeBSD, NetBSD, OpenBSD, embedded Linux, WinCE, Haiku, OpenWRT, iPhone (iOS), Android, Nintendo Wii and Gamecube through DevKitPro, QNX, MontaVista, OpenCL, NonStop, TRON/ITRON/ $\mu$ ITRON, Micrium's  $\mu$ C/OS, FreeRTOS, SafeRTOS, Freescale MQX, Nucleus, TinyOS, HP/UX, ARC MQX, TI-RTOS

- If you would like to test wolfSSH on another environment, let us know and we'll be happy to support you.

[www.wolfssl.com](http://www.wolfssl.com)

Copyright © 2017 wolfSSL Inc. All Rights Reserved