

# OpenSSH 4.2 released

*LR*

OpenSSH allows you to login to remote systems and use them as if they were your local system, easily copy files to one place to another and is probably the best thing since sliced bread. The new version has some security fixes, the default key size is now 2048 bits and now supports X11 forwarding over multiplexed connections.

---

Changes since OpenSSH 4.1:

---

- **SECURITY:** Fix a bug introduced in OpenSSH 4.0 that caused GatewayPorts to be incorrectly activated for dynamic ("-D") port forwardings when no listen address was explicitly specified.
- **SECURITY:** sshd in OpenSSH versions prior to 4.2 allow GSSAPI credentials to be delegated to users who log in with methods other than GSSAPI authentication (e.g. public key) when the client requests it. This behaviour has been changed in OpenSSH 4.2 to only delegate credentials to users who authenticate using the GSSAPI method. This eliminates the risk of credentials being inadvertently exposed to an untrusted user/host (though users should not activate GSSAPIDelegateCredentials to begin with when the remote user or host is untrusted)
- Added a new compression method that delays the start of zlib compression until the user has been authenticated successfully. The new method ("Compression delayed") is on by default in the server. This eliminates the risk of any zlib vulnerability leading to a compromise of the server from unauthenticated users. NB. Older OpenSSH (<3.5) versions have a bug that will cause them to refuse to connect to any server that does not offer compression when the client has compression requested. Since the new "delayed" server mode isn't supported by these older clients, they will refuse to connect to a new

server unless compression is disabled (on the client end) or the original compression method is enabled on the server ("Compression yes" in sshd\_config)

- Another round of proactive changes for signed vs unsigned integer bugs has been completed, including changing the atomicio() API to encourage safer programming. This work is ongoing.
- Added support for the improved arcfour cipher modes from draft-harris-ssh-arcfour-fixes-02. This improves the cipher's resistance to a number of attacks by discarding early keystream output.
- Increase the default size of new RSA/DSA keys generated by ssh-keygen from 1024 to 2048 bits. including: -Added ControlMaster=auto/autoask options to support opportunistic multiplexing (see the ssh\_config(5) manpage for details). -The client will now gracefully fallback to starting a new TCP connection if it cannot connect to a specified multiplexing control socket -Added %h (target hostname), %p (target port) and %r (remote username) expansion sequences to ControlPath. Also allow ControlPath=none to disable connection multiplexing. -Implemented support for X11 and agent forwarding over multiplexed connections. Because of protocol limitations, the slave connections inherit the master's DISPLAY and SSH\_AUTH\_SOCK rather than distinctly forwarding their own.
- Portable OpenSSH: Added support for long passwords (> 8-char) on UnixWare 7. -Lots of other improvements and fixes. Please refer to the ChangeLog for details
- The following bugs from <http://bugzilla.mindrot.org/> were closed:

```
#471-Misleading error message if /dev/tty perms wrong
#623-Don't use $HOME in manpages
#829-Don't allocate a tty if -n option is set
#1025 - Correctly handle disabled special character in tty mode
#1033 - Fix compile-time warnings
#1046 - AIX 5.3 Garbage on Login
#1054 - Don't terminate connection on getpeername() failure
#1076 - GSSAPIDelegateCredentials issue mentioned above
```

---

Learn more:

- [OpenSSH](#)
- [Mailing list announcement](#)
- [SSH Usage Tips](#)

OpenSSH Manual pages:

- [sshd](#)
- [ssh](#)

---

> [Linux Reviews](#) > [News and headlines](#) > [2005 News archive](#) > [September](#)  
>  
OpenSSH 4.2 released