

OSTG | ThinkGeek - Slashdot - ITMJ - Linux.com - NewsForge - freshmeat - Newsletters - PriceGrabber - Jobs - Broadband - Whitepapers

Ads by Google

SSH Server for Windows
Fine tune control. Easy setup.
Download VShell today!
www.vandyke.com

SSH Telnet for Windows
AnzioWin, reliable secure network
connections with advanced features.
www.anzio.com

SSH for Windows
Advanced SSH client & server suite:
terminal, tunneling, file transfer
www.bitvise.com

SSH Client for Windows
Secure terminal and tunneling.
Download Free Trial Now!
RemotelyAnywhere.com


[my sf.net](#)
[software map](#)
[donate to sf.net](#)
[about sf.net](#)

welcomes [gballego](#) (Logout)

[Register New Project](#)

[Search](#)

This Project



Search

results by **YAHOO!** search

SF.net Subscription

- [Subscribe Now](#)
- [Manage Subscription](#)
- [Realtime Statistics](#)
- [Direct Download](#)
- [Priority Tech Support](#)
- [Project Monitoring](#)

SF.net Resources

- [Site Docs](#)
- [Site Status](#) (06/14)
- [SF.net Supporters](#)
- [Compile Farm](#)
- [Project Help Wanted](#)
- [New Releases](#)
- [Get Support](#)

Site Sponsors

TigerDirect.com
Search for deals on
BAREBONES

Bring
SOURCEFORGE
INTO YOUR ENTERPRISE

Learn &
Download
DB2 [Click Here](#)

ThinkGeek

Most Active

Project: SourceForge.net: Document Manager: Display Docu

[Summary](#) | [Admin](#) | [Home Page](#) | [Forums](#) | [Tracker](#) | [Support](#) | [RFE](#) | [Lists](#) | [D](#)

[Submit new documentation](#) | [View Documentation](#) | [Admin](#) | [Search Site Doc](#)

Guide to Generation and Postir





This document provides instructions for project developers to use in genera SSH public key to SourceForge.net. The use of SSH keys allows password server, project CVS server, and SourceForge.net Compile Farm.

Team Members

(Developers) Only This document has been designed for use ONLY by Sourc team (i.e. listed active developers on a project, in the team member list for that prc are a project developer, affiliated with a project and listed on their development te information in this document likely does not apply to you.


[Table of Contents](#) » | [doc feedback](#) | [support](#)

- [SSH: SourceForge.net hosts](#)
- [SSH: The purpose of SSH](#)
- [SSH: Authentication by shared keys](#)
- [SSH: Key types](#)
- [SSH: Importance in protecting SSH private key data](#)
- [SSH: SSH clients](#)
- [SSH key generation: PuTTY](#)
- [SSH key generation: OpenSSH](#)
- [SSH key posting: Form for posting keys](#)
- [SSH key posting: Supported key formats](#)
- [SSH key posting: Importance of using our upload form](#)
- [SSH key posting: Keeping multiple keys on file](#)
- [SSH key posting: Invalidating unused keys](#)
- [SSH key posting: Sync delay](#)
- [SSH key passphrases: Usage](#)

- 1 Azureus - BitTorrent Client 
- 2 Gaim
- 3 Compiere ERP + CRM Business Solution
- 4 7-Zip
- 5 phpMyAdmin 
- 6 FCKeditor
- 7 PDFCreator 
- 8 ScummVM 
- 9 AMSN
- 10 FileZilla 

[More Activity>>](#)

Top Downloads

- 1 Azureus - BitTorrent Client 
- 2 eMule
- 3 MinGW - Minimalist GNU for Windows
- 4 BitTorrent
- 5 DC++
- 6 GTK+ and The GIMP installers for Windows
- 7 Gaim
- 8 NASA World Wind
- 9 VirtualDub
- 10 Shareaza

[More Statistics>>](#)

SF.net Services

- [Jobs](#)
- [PriceGrabber](#)
- [Whitepapers](#)
- [Partner Product Offers](#)
- [Get Broadband](#)
- [IT Product Guide](#)

Sponsored Content

- [SSH key passphrases: Changing your passphrase under PuTTY](#)
- [SSH key passphrases: Changing your passphrase under OpenSSH](#)
- [SSH authentication agents: Overview](#)
- [SSH authentication agents: PuTTY's PAGEANT](#)
- [SSH authentication agents: OpenSSH's ssh-agent](#)
- [Using SSH keys: Setting your preferred SSH protocol version](#)
- [Using SSH keys: Generating replacement keys](#)
- [Using SSH keys: Backing up your SSH key data](#)
- [Using SSH keys: Copying SSH key data between hosts](#)
- [Using SSH keys: Coping with lost SSH keys](#)
- [Using SSH keys: Regenerating a lost SSH public key](#)
- [Using SSH keys: What does SSH key data look like?](#)
- [Support](#)

[^ SSH: SourceForge.net hosts »](#) | [doc feedback](#) | [support](#)

SourceForge.net provides to project developers a number of services which called SSH (Secure SHell).

These services include:

- **shell.sf.net**: Project shell service, used to generate and maintain we provided to all project members (developers).
- **cv.ssf.net**: Project CVS service, used to securely access and write t This service is provided to all project members (developers).
- **cf.sf.net, cf-shell.sf.net**: Compile Farm service, used for testing of s software building. This service is provided to all project members (de [Maintenance page](#).

Reference: [Introduction to SSH at SourceForge.net](#), [Project shell server do developers](#), [Guide to the SourceForge.net Compile Farm](#)

[^ SSH: The purpose of SSH »](#) | [doc feedback](#) | [support](#)

SSH (Secure SHell) is a secure replacement for TELNET (used to access h RSH/REXEC (used to execute programs on a remote host), and FTP (used TELNET, RSH/REXEC and FTP all send password data in a way that can € uses encryption to protect both your login to a system and the data you sen provide support for TELNET, RSH/REXEC or FTP to the shell, CVS and co

Reference: [Introduction to SSH at SourceForge.net](#), [Why can't I use TELNE hosts?](#)

[^ SSH: Authentication by shared keys »](#) | [doc feedback](#) | [support](#)

The SSH protocol includes a provision to allow you to login to hosts using a method of passwords. When using shared keys, a private key (which you g secure token that only you have, and a public key (derived from the private servers. When you connect to the remote server, data generated against yc against your public key. The handshake used to authenticate you to a serve much more secure than the use of passwords.

[^ SSH: Key types »](#) | [doc feedback](#) | [support](#)

Over the years, the SSH protocol has been redesigned several times; each of keys. The SSH1 protocol supports RSA keys; the SSH2 protocol support supports both the SSH1 and SSH2 protocols, RSA and DSA keys.

SourceForge.net maintains two sets of SSH keys for each user. One set is the project shell (shell.sf.net) and CVS servers (cvs.sf.net). The second set Compile Farm (cf.sf.net and cf-shell.sf.net). All SSH key data is managed u [Maintenance page](#) on the SourceForge.net site.

[^ SSH: Importance in protecting SSH private key data »](#) | [doc feedback](#) | [support](#)

Only public key data should ever be uploaded to SourceForge.net. Private keys should be protected properly, both in terms of preventing unwanted access to the keys and should be protected properly, both in terms of preventing unwanted access to the keys through the use of a passphrase on all SSH private keys (unless used for a service that require you to login (including the SourceForge.net web site, s service) should only be accessed from secure, trusted machines.

[^ SSH: SSH clients »](#) | [doc feedback](#) | [support](#)

A SSH client is needed in order to connect to a host using the SSH protocol. The following Open Source SSH clients:

On Microsoft Windows platforms, [PuTTY](#) and [WinSCP](#) (WinSCP is hosted c support for SSH (used for interactive login), SCP and SFTP (used for file tra

On UNIX platforms (such as BSD and Linux) and Mac OS X, [OpenSSH](#) pro clients. Mac OS X, and most BSD and Linux distributions include OpenSSH. On Microsoft Windows platforms as part of the Cygwin suite.

Reference: [Recommended client software configuration](#)

[^ SSH key generation: PuTTY »](#) | [doc feedback](#) | [support](#)

1. Execute PUTTYGEN.EXE
2. Select the desired key type ("SSH2 DSA", within the "Parameters" se



3. Click on the "Generate" button.
4. Follow the on-screen instructions ("Please generate some randomne area"). Key generation will be performed immediately afterward.
5. Enter username@shell.sf.net (or username@cf.sf.net) in the "Key co your SourceForge.net user name. This comment will help you to ider
6. Enter the desired [passphrase](#) in the "Key passphrase" and "Confirm



7. Click on the "Save private key" button; use the resulting dialog to save. You may use a filename such as "SourceForge-Shell.ppk" or "SourceForge-Shell Private Key files."



8. Go to the [SSH key posting page on the SourceForge.net site](#). Copy and paste into OpenSSH authorized_keys2 file" section of the PuTTY Key form on the SourceForge.net site.



9. Exit the PuTTY Key Generator.

Reference: [PuTTY manual: Using public keys for SSH authentication](#)

[^] **SSH key generation: OpenSSH** » | [doc feedback](#) | [support](#)

Please use a [passphrase](#) to protect your key.

```
$ ssh-keygen -t dsa -C "username@shell.sf.net"
Generating public/private dsa key pair.
Enter file in which to save the key (/home/username/.ssh):
Created directory '/home/username/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/username/.ssh/id_dsa.
Your public key has been saved in /home/username/.ssh/id_dsa.pub.
The key fingerprint is:
f3:31:a8:c6:82:18:c8:0f:dd:6b:fb:27:98:83:3d:3b username@shell.sf.net
```

Key types (specified using the -t flag on the command-line) include: rsa1 (SSH1/RSA), rsa (SSH2/RSA), dsa (SSH2/DSS), ecdsa (SSH2/ECDSA), and ed25519 (SSH2/Ed25519).

We recommend that you use a comment of username@shell.sf.net (or your SourceForge.net user name). This comment will help you to identify the key.

Reference: [ssh-keygen manual page](#)

^ SSH key posting: Form for posting keys » | [doc feedback](#) | [support](#)

SourceForge.net allows you to use a separate set of SSH keys for the project shell service. SourceForge.net Compile Farm service. We strongly recommend that you use a separate set of SSH keys as you use for the Compile Farm (this is an added security feature that should not be shared). SSH keys may be found on the [Account Maintenance page](#) (the Compile Farm section is only present if you have opted-in for Compile Farm access).

OpenSSH users will upload the contents of their id_dsa.pub (used for SSH2/DSS) and id_rsa.pub (used for SSH2/RSA) files (as needed, based on the type of key you specify SSH2/DSS, so your key would be placed in ~/.ssh/id_dsa.pub by default). These files store the public key data. Private key data should never be uploaded.

PuTTY users will paste to the form the contents of the "Public key for pasting" section of the PuTTY Key Generator (PUTTYGEN.EXE) after loading their key.

^ SSH key posting: Supported key formats » | [doc feedback](#) | [support](#)

SourceForge.net supports SSH1 RSA keys, SSH2 RSA and DSA keys which are OpenSSH-compatible. Both OpenSSH and PuTTY generate key data which is OpenSSH-compatible.

Keys generated using recent versions of the SSH Communications, Inc. Secure Shell (SSH) IETF SECSH key file format, will need to be converted to an OpenSSH-compatible format. SourceForge.net. The OpenSSH 'ssh-keygen' utility's '-i' option provides a simple way to convert keys.

From the ssh-keygen manual page:

```
ssh-keygen -i [-f input_keyfile]
```

```
-i      This option will read an unencrypted private key in SSH2-compatible format and print an OpenSSH Public Key File Format'. This option allows conversion of several commercial SSH implementations.
```

PuTTY's PUTTYGEN.EXE also allows you to import keys and export them in OpenSSH-compatible format.

^ SSH key posting: Importance of using our upload form » | [doc feedback](#) | [support](#)

While it is possible to directly place SSH key data on the project shell service, we strongly recommend that you use our SSH key management pages on the SourceForge.net site, accessible from the project shell service. Data placed on any SourceForge.net hosts may be overwritten at any time without notice. By using our upload form, you ensure your SSH key is stored securely. You can easily check to see which keys are active using the provided web interface. If we were to begin providing a new service based on SSH, we would already have your keys.

^ SSH key posting: Keeping multiple keys on file » | [doc feedback](#) | [support](#)

You may keep multiple SSH keys on file (even one or more of each format SSH1, SSH2, and SSH2/RSA). When uploading your SSH key data, one line should be used for each key.

^ SSH key posting: Invalidating unused keys » | [doc feedback](#) | [support](#)

You should only keep keys on file with SourceForge.net if they are actively used. If you have removed a key from your SSH key profile on the SourceForge.net site, you should remove it from your local machine. To invalidate a key, go to the SSH key management page for the service in question (CVS/shell or Compile Farm) and re-post the keys you want to continue using (leave out the key you want to invalidate).

^ SSH key posting: Sync delay » | [doc feedback](#) | [support](#)

There is presently up to a 10 minute delay between the time SSH keys are added to your profile and they are synchronized to the project shell and CVS servers, or SourceForge.net. This delay is usually a few minutes before reporting an issue with the key sync process. Any temporary delays (due to upgrades and outages) will be listed on the [SourceForge.net Site Status](#) page.

^ SSH key passphrases: Usage » | [doc feedback](#) | [support](#)

SSH clients such as PuTTY and OpenSSH allow you to set a passphrase on your private key. When you set a passphrase on your private key, the SSH client will ask you to enter that passphrase when you connect to a remote host using that key. This is added security to protect your identity if they were to steal your SSH private key. This passphrase is used to encrypt the private key and is not transmitted over the wire.

SourceForge.net encourages you to always place a passphrase on your SSH private key. This is especially important if you are using a single, secure machine in an automated application (such as launching a Compile Farm each night).

^ SSH key passphrases: Changing your passphrase under PuTTY » | [doc feedback](#)

1. Run PUTTYGEN.EXE
2. Click on the "Load" button.
3. Select the file which contains your private key.
4. Enter the existing passphrase for the private key when prompted.
5. Enter the new desired passphrase in the "Key passphrase" and "Confirm passphrase" fields.
6. Click on the "Save private key" button. Overwrite the existing copy of the private key.

Reference: [PuTTY manual: Reloading a private key](#)

^ SSH key passphrases: Changing your passphrase under OpenSSH » | [doc feedback](#)

```
$ ssh-keygen -p -t dsa
Enter file in which the key is (/home/username/.ssh/id_dsa)
Enter old passphrase:
Key has comment '/home/username/.ssh/id_dsa'
Enter new passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase
```

^ SSH authentication agents: Overview » | [doc feedback](#) | [support](#)

Many developers leave their workstation on for the whole work day, or several time period, you may perform a large number of SSH operations, particularly SSH.

Most SSH clients provide an authentication agent to save you from having to enter your passphrase each time you access a host with that key. Both PuTTY and OpenSSH include an authentication agent at time of login or system startup, then add your keys to the agent (or the key at that time). When you connect to a host, SSH checks with the authentication agent for your private key but with added convenience (you only need to enter your passphrase once to the authentication agent).

^ SSH authentication agents: PuTTY's PAGEANT » | [doc feedback](#) | [support](#)

1. Run PAGEANT.EXE



2. Access the Pageant Key List via the Pageant button in the System Tray.
3. Click on the "Add Key" button.
4. Select the file which contains your private key.



5. Enter the passphrase for your private key when prompted. The selected key will be added to the Pageant Key List.



6. Close the Pageant Key List dialog using the Close button.
7. PuTTY and WinSCP will now be able to use the provided key automatically without prompting for the passphrase (until Pageant is shut down, or your machine is rebooted).

Reference: [WinSCP documentation on connecting to remote hosts](#)

^ SSH authentication agents: OpenSSH's ssh-agent » | [doc feedback](#) | [support](#)

Many OS distributions that include OpenSSH are configured to automatically (in the background) upon login. Once 'ssh-agent' is running, you may add your key specified on the command-line, the keys in that file will be added; if not, ssh identity files in your .ssh directory) command.

```
$ ssh-add
Enter passphrase for /home/username/.ssh/id_dsa:
Identity added: /home/username/.ssh/id_dsa (/home/user

$ ssh-add -l
1024 f3:31:a8:c6:82:18:c8:0f:dd:6b:fb:27:98:83:3d:3b /
```

After adding your SSH key to the SSH agent, OpenSSH-based tools ('ssh', without prompting you for the passphrase (as long as the SSH agent remain

[^ Using SSH keys: Setting your preferred SSH protocol version »](#) | [doc feedback](#)

The SSH protocol version (SSH1 vs. SSH2) of your generated SSH key pair is stored in the key file. Your SSH client to use in order for the keys to be used.

Under OpenSSH, the preferred protocol version may be specified globally (in /etc/ssh/sshd_config) or locally (in ~/.ssh/config). (or similar, depending on where this file is stored in your OS distribution). OpenSSH can be used to specify either SSH2 or SSH1 as the preferred protocol (respectively).

```
Protocol 2,1
Protocol 1,2
```

Under OpenSSH, you may also specify the preferred SSH protocol version flags to 'ssh'.

Under PuTTY's command-line PLINK.EXE utility, preferred SSH protocol version flags to 'PLINK.EXE'.



[^ Using SSH keys: Generating replacement keys »](#) | [doc feedback](#) | [support](#)

As you regularly change passwords on your user accounts, you should also change your SSH passphrase).

[^ Using SSH keys: Backing up your SSH key data »](#) | [doc feedback](#) | [support](#)

You are solely responsible for ensuring you have a viable backup of your SSH key data. Your SSH key should be treated with the same level of security and paranoia that you treat your source code. Security should be the first and last thing you consider when backing up sensitive data.

Backups of your SSH key data may not be necessary; if your SSH key is lost, simply generate a new one and invalidate the old one. If you decide you do want to backup your SSH key data, do so securely.

OpenSSH users should backup the contents of the `.ssh` subdirectory of their home directory (not on the shell server).

PuTTY users should backup their key data.

Backups should not be shared between users; if a key is lost, simply invalidate it and generate a new key to replace the lost key.

[^ Using SSH keys: Copying SSH key data between hosts »](#) | [doc feedback](#) | [support](#)

As SourceForge.net permits you to have multiple keys (even of the same type), there is a little reason to copy SSH key data between different hosts. We encourage you to backup your hosts (as to minimize security impact).

SSH key data may be backed up and restored in the event that you reload your key or generate a new SSH key and invalidate your old key. If you decide to generate a new key, be sure to invalidate any disused keys.

[^ Using SSH keys: Coping with lost SSH keys »](#) | [doc feedback](#) | [support](#)

If you lose your SSH private key data, take steps to immediately invalidate it. There is no facility. Regenerate and post a replacement SSH key, if needed. If your key is lost, you should notify the other members of your development team and verify the integrity of the code.

[^ Using SSH keys: Regenerating a lost SSH public key »](#) | [doc feedback](#) | [support](#)

If you have lost your SSH public key, but still have the SSH private key, you can use the SSH client suite to derive the public key from the private key data.

When using OpenSSH, you may print the public key matching a private key

```
$ ssh-keygen -t dsa -y
Enter file in which the key is (/home/username/.ssh/id_dsa)
Enter passphrase:
ssh-dss AAAAB3NzaC1kc3MAAACBApuPDda/vM44njJfOyFyndlnOvn
Ez6pB7u0ZH9nPvfNwaxfPFejaHvOgexct8vkQ5gavY7tjOe19ujWkj
/P39L+/ffkJ5SNdoHJVC8bfpXhukwQxlFFdOYfoJAAAAFQDiomSqQX
byiu9vyqC6cRRaUWu5jsjxUv+dzcOlJyG1LW1kSmV8127qQvy/n9gF
Lk2fVu93xvN7rzdT6xRLuqNzSGnGuqo00ldg6JU+XyHTdNksOBDNz0
z2STJZSZdAAAAIBEG6g8HQEZhyC8uaDYNk/23FUBTQp++NVWHcSP6g
F2gnhB/0Y5XHEjE9jhFoEyDgBF3U1NksILVcNX6jMBxepFgHtkV+CG
aGapXaVYwZpTUpiuQQyYxb/o+w==
```

When using PuTTY:

1. Run PUTTYGEN.EXE
2. Click the "Load key" button.
3. Select the file which contains your private key.
4. Enter the passphrase for your private key when prompted.
5. The matching public key will be displayed in the "Public key for pasting" section of the PuTTY Key Generator and may also be saved to file.
6. The PuTTY Key Generator also provides the ability to export key data in the OpenSSH public key format.



[^] [Using SSH keys: What does SSH key data look like?](#) » | [doc feedback](#) | [support](#)

Sample SSH1 (RSA) key data (data is on one line, normally, but has been l

```
1024 35 1416172998593696062015943071487167622332918714
412742462887905399790197899584622819338390620554068654
802732791005548972423681429393496791918739196652091521
703209675908129656993535418633951314772546759474382936
username@hostname.localdomain
```

Sample SSH2 (DSA) key data (data is on one line, normally, but has been l

```
ssh-dss AAAAB3NzaC1kc3MAAACBAN431nwhJuE5F5HhsTVS7WlSCH
XbsLjKIBz2P/jaL2w92U72cUmKiXgVFaxP7LgRylF0UHjFoPfbbesY
f62q0mPIZQxyq6SSyqLD6NiO3IlyrsCSXAerkrdxAAAAFQD7wt2MuZ
vQvsiBcgEVvlAIMnZlP2QdO2O96p0wlCoHmKS8WYhwiAEB4QsLypM9
pOMKAWVJSsuJqqH0VBLHZVD5tdBPG4p4i3uws6my2z2AQARMfKN9L/
xZInM/hFrVcAAACBAL9K78gikerCL/LFLK4FkQp56drqx2WmubrAuG
540XW0PYDz53NnBc3C3/v3EE4nokyyUw783mWKbAbI6+jtibViUhfJ
zFyjC4Db4UrmU71tYQfOlzmIipf7 username@hostname.localdo
```

SSH key data should not be modified during the upload process; do not add spaces during the upload process.

[^] [Support](#) » | [doc feedback](#) | [support](#)

The SourceForge.net support team is happy to assist with any issues related to the SourceForge.net support team, first login to the SourceForge.net web site, then be logged-in when submitting issue reports related to the use of SSH keys.

[Return to the top of this page.](#)

© Copyright 2002-2004 Open Source Development Network. All rights reserved.

Powered by SourceForge® collaborative software development tools from VA Software

© Copyright 2005 - OSTG Open Source Technology Group, All Rights Reserved

[About SourceForge.net](#) • [About OSTG](#) • [Privacy Statement](#) • [Terms of Use](#) • [Advertise](#) • [Get Support](#)

ITManagersJournal--Spot emerging business trends with news and product reviews for enterprise IT.