Tools to Generate SSH Keys

This Page is a work in progress

Bitvise SSH Client

BitVise SSH Client Tunnelier is the recommended client for key generation on Windows.

Generating your private key:

Open BitVise SSH Client Tunnelier.

Click in "Client Key Manager"

🚿 Bitvise SSH Cli	ent 7.35 — 🗆 🗙
Profile: test.tl	p Closing behavior
Load profile Load profile Save profile Save profile as	Login Options Terminal Remote Desktop SFTP Services C2S S2C SSH About Server Host
Close profile	Proxy settings Host key manager Client key manager Help 15:06:26.000 Current date: 2017-11-22 15:06:26.000 Bitvise SSH Client 7.35, a fully featured SSH client for Windows. Copyright (C) 2000-2017 by Bitvise Limited. 15:06:26.000 Visit www.bitvise.com for latest information about our SSH software. 15:06:26.000 Run 'BvSsh -help' to learn about supported command-line parameters. 15:06:26.000 Cryptographic provider: Windows CNG (x86) with additions 15:06:26.342 Loading last used profile 'C:\Users\gmagella\Documents\test.tp'. 15:06:26.343 Last used profile loaded successfully.
	Login Exit

Click on GENERATE NEW:

u have the	following SSH user	authentic	ation keys:					
ocation	Algorithm	Size	Pass	MD5 Fingerprint	Bubble Babble	SHA-256 Fing	gerprint	Comm

Select RSA, Size: 4096 and (Optionally) enter a good passphrase.

Note: this passphrase will give anyone access to our private key, it's recommended that you keep it safe in some sort of encrypted vault like Keepass.

Bitvise Cl	ient Key Managem	ent Ci	Generate New Keypair			×		-		\times
Client Ke You have the Location	y Manager following SSH user a Algorithm	uthentica Size	Location Profile 1 Passphrase Confirm passphrase The client key will not b passphrase is supplied. Comment	Algorithm RSA pe passphrase protection	•• ed if an	Size 4096 V empty	-256 Fingerprint		Comm	ient
٢			Generated by user@C	rate Cancel		< >	Modif Change Pas	y sphrase	Remov	> 'e •

After you generate it, you should export the public key and private keys

Export the private key in the proper format:

Click in Export, Select "Export private key" and "PuTTY format"

						Export Public o	r Private K	iey	×	
Bitvise Client Client Key M You have the follow	Key Management anager wing SSH user authenti	Cryptograph	ic provider: Windows C	:NG (x86) with addition	5	C Export publi Export the public Standard OpenSS	ic key blic key for d SSH2 for H format	import on an SSH serve mat	r.	×
Location A	lgorithm Size	e Pass	MD5 Fingerprint	Bubble Babble	SHA-256 F	Export priva	ate key			
Client keys su	pported by the currer	nt crypto pro	vider (1):			Export the priv another machin	vate key f	or backup or for use on erent SSH client.		
Profile 1 R	ISA 405	96 yes	7e:0e:d0:e1:b2:d8:	xigar-fadad-kacof-b	/ozJA5gpV	O Bitvise f	ormat			NAME.
						OpenSS	H format			
						PuTTY fi	ormat			
<					_	E	xport	Cancel		>
Comment:	Generated by user	COMPUTER	NAME.						_	
MD5 fingerprint:	7e:0e:d0:e1:b2:d8	8:4a:18:27:b2	:a1:08:33:cf:99:b3			Generate	New	Modify	Re	move
Bubble-babble: SHA-256 fingerprir	xigar-fadad-kacof- nt: /ozJA5gpW63U4P8	benez-gocyf- 3pkR9GCa4dR	pabik-henyh-suzip-hudop i99Hp0jE9cUd/LnEsA	-mepak-cyxax		Import	Export	Change Passphrase	M	ore 🔻

NOTE: Do not share this file with anyone. This is your identity

Enter the passphrase for the key and make sure "Use Existing Passphrase" is selected so the key will be passphrase protected.

Point to a directory and save the file.

Next, lets import it to use in PuTTYNG for use with mRemoteNG.

Click on Tools, Options.

mRemoteNG - confCons.xml							
File View	Тоо	ls Help Connect:					
Connections	3\$	SSH File Transfer					
😫 📮 🖮	•	External Tools					
🖻 🚱 DMTS		Port Scan					
È-È AEM È-È IST	÷	Components Check					
−	Þ	Options					



🎲 mRemoteNG Options		
Startup/Exit Appearance Tabs & Panels Connections SQL Server Updates Theme	 Write log file (mRemoteNG.log) Automatically get session information Automatically try to reconnect when disconnected from server (RDP Use custom PuTTY path: 	& ICA only) Browse
U Security	To configure PuTTY sessions click this button: Maximum PuTTY and integrated external tools wait time:	Launch PuTTY

Scroll down, expand Connection -> SSH - > Auth and click in "Browse" to locate your private key.

🎲 mRemoteNG Options						
📓 Startup/Exit	Write log file (mRemoteNG.log)					
Appearance	Automatically get session information					
Connections	Automatically try to reconnect when disconnected from server (RDP & ICA only)					
SQL Server	Use custom PuTTY path:					
📥 Updates	Browse					
1 Theme						
Security						
age Advanced	To configure Pully sessions click this button: 💦 Launch Pully					
	Maximum PuTTY and integrated external tools wait time: 2 🔹 seconds					

Scroll back up and click on Session.... Select Default Session and click SAVE.

Optionally you can set up another Session Name, so you wouldn't change your default session settings.

Optionally you can also load a session and save it with another name so you can change only a few configuration. E.g. change the background of SSH for production servers for improved awareness.

Optional Step: set logging for audit purposes:

Go to Session...Logging

On the first section select "Printable output"

On Log file name type: <ROOT_FOLDER>\SSH\LOGS\putty_&Y&M&D&T_&H.log

Note: please replace <root_folder> by a location/folder on your computer, ex: "e:\SSH"

Check "Always append to the end of it" for existing log files.

```
Check "flush log file frequently".
```

Click back in "Session", select "Default Settings" and click in SAVE.

Properly exporting the Public Key

Your public key is the key you want to share with the server owner, so SSH will be able to authenticate you.

In Bitvise you can export two types of public keys,

- 1. Standard SSH2 format This is for the Bitvise client
- 2. OpenSSH format This is for adding to servers for access

This export option can be found by opening Bitvise selecting the User keypair manager.

😴 Bitvise SSH Clier	nt 4.62									• ×
Profile: digital.	bscp (cl	anged)								
	Login	Options	Terminal	Remote Desktop	SFTP	Services	C2S	S2C	SSH	About
Load profile	Serve	r			Auth	entication –				
	<u>H</u> ost				<u>U</u> se	rname				
23	Port Prov	22 ov settings	Hos	t key manager	Initi	al <u>m</u> ethod	publick	ey - slot	1	•
Save profile	SDN		103	servey manager	Pas	sphrase				
2		SDI Kerbe	ros 5	Delegation	Use	r keypair m	anager			
Save profile as		SFINCIDE		Delegation	1	Try gssapi-ł	keyex fir	st if avai	lable	
٠										
Close profile										Help
	 09:04 09:04 09:04 09:04 09:04 09:04 09:04 	4:32.032 4:32.032 4:32.032 4:32.495 4:32.500	Bitvise SSH Copyright (Portions Co Visit www.b Run 'BvSsh Loading las Last used p	Client, a fully feat. (C) 2000-2013 by B ppyright (C) 1995-2 pitvise.com for lates - help' to learn the t used profile 'C: \Us profile loaded succe	red SSH tvise Lim 003 by W st informa supporte sers \Rod ssfully.	2 client. ited. /ei Dai. ation about d command erick\Docun	our SSH I-line par nents\dig	2 produc ameters gital.bscp	:ts. '.	
		Login							Exi	t

Select the Key you want to export and click Export...

ou hav	e the followir	ng SSH u	iser auther	ntication keypairs:			
Slot	Algorithm	Size	Pass	MD5 Fingerprint	Bubble Babble	Insert Time	Comment
5	ssh-rsa	2048	no	d4:ea:ba:03:c0	xitas-palib-pysy	2017-09-08T13:21:37Z	Generated by Roderick@pcname.

Select OpenSSH format and click Export



Name the file and save it.

Select OpenSSH Public Key Export File				×
→ Roderick → Desktop → New folder (2)		▼ 4 9 Se	arch New folder (2)	م
Organize 🔻 New folder			:== :==	• 🕡
Name ^	Date modified Type	e Size		
E	No items match your sea	rch.		
-				
La Carteria de Car				
-				
File name: testpublickey				-
Save as type:				-
Hide Folders			Save	Cancel

Send the file or the contents to the Server Administrator to add your key onto ~/.ssh/authorized_keys

Puttygen

It is not recommended to use Puttygen to generate keys. The software has not been updated in a very long time. Instead, for Windows, look at BitVise SSH Client Tunnelier or a current Unix/Linux system.

Run the puttygen.exe if you do not have it you can download it here.

Here you can change the key type and length for this example we will use default. For more information on industry standards refer to this page.

😴 PuTTY Key Generator	? 💌
<u>File Key Conversions Help</u>	
Key No key.	
Actions Generate a public/private key pair	Generate
Load an existing private key file	Load
Save the generated key	Save public key Save private key
Parameters	
Type of key to generate: SSH-1 (RSA)	SSH-2 DSA
Number of bits in a generated key:	2048

Click Generate and follow the instructions of moving your mouse in the space till the bar is filled.

PuTTY Key Generator					? ×
ile <u>K</u> ey Con <u>v</u> ersions <u>H</u>	elp				
Key Please generate some random	nness by moving	the mouse over t	the blan	k area.	
Actions Generate a public/private key	pair			Gene	arate
Load an ovisting private logufi	la			Le.	
Save the generated key		Save public k	(ey	Save priv	vate key
Parameters					
Type of key to generate: SSH- <u>1</u> (RSA)	SSH-2 <u>R</u> SA		SSH	-2 <u>D</u> SA	
Number of bits in a generated	key:			2048	

Once finished your public key will be displayed as well as some options to set a passphrase and save your keys. The box at the top is your public key that you would copy into your authorized_keys file in the ssh directory. You can also save the public key and send it to others to grant you access to servers.

😴 PuTTY Key Generato	r	? 🔀	
<u>File Key Conversion</u>	s <u>H</u> elp		
Key			
Public key for pasting in	to OpenSSH authorized_keys file:		
ssh-rsa AAAAB3NzaC1yc2EA /ANXT4/cKdHVwRgv LUXwQKSX4Gh4ThQ ZofKfnoFFfK4GsapT5	VAABJQAAAQEAkgaHzfLMh1MvR6XNuzuDg /UEhYwCjo4GieRw0nsjOlny3Xnhx5CaBbzBX Qg3V4SIMAqbZQ5/qT/8kmgDVdbhuL/eV40 8bW4iq2SOZOTqIrsPyh/n6SZS6oqBxjdCD7	DB1j4JPfRAAT26 fLx1y1YsUrXAJ0K ZloVg0xMN5X3Vti 1YVO00MJr2FORI	
Key fingerprint:	ssh-rsa 2048 e8:94:e5:e5:7a:2e:20f1:2b:9b:65:c1:76:88:7d:14		
Key comment:	bobsrkey-20170324		
Key passphrase:	•••••		
Confirm passphrase:	•••••		
Actions			
Generate a public/priva	te key pair	<u>G</u> enerate	
Load an existing private	key file	Load	
Save the generated ke	Save public key	Save private key	
Parameters			
Type of key to generate SSH- <u>1</u> (RSA)	e:	H-2 <u>D</u> SA	
Number of bits in a gen	erated key:	2048	

Note when you save the private key its in format ".ppk"(Putty Private Key) this will only work in the putty client. If you need a private key without the putty format you can find it under Conversions.

e Key	Conversion	s Help			
Key	Import key Export OpenSSH key Export ssh.com key				
Public ke ssh-rsa			ys file:	ys file:	
AAAAB3 /ANXT4			n1MvR6XNuzuDgDB1j4JPfRAAT26 3Xnhx5CaBbzBXfLx1v1YsUrXAJ0K		
LUXwQK ZofKfnoF	SX4Gh4ThQ FfK4GsapT55	2g3V4SIMAqbZQ5/q 8bW4iq2SOZOTqlrsF	T/8kmgDVdbhuL/eV402 Pyh/n6SZS6oqBxjdCD7	ZoVgOxMN5X3VtI IYVOO0MJr2FORI ←	
Key fingerprint:		ssh-rsa 2048 e8:94:e5:e5:7a:2e:20f1:2b:9b:65:c1:76:88:7d:14			
Key comment:		bobsrkey-20170324			
Key p <u>a</u> ssphrase: C <u>o</u> nfim passphrase:		••••••			
					Actions
Generate	a public/priva	te key pair		Generate	
Load an existing private key file				Load	
Save the	generated key	(Save p <u>u</u> blic key	Save private key	
Parameter	rs				
Type of k	ey to generate (RSA)	:	A 💿 SSI	1-2 <u>D</u> SA	

The location to load your key in the putty client is in Auth on the left side scroll down and select Auth then browse for you key.

